LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

ISO 28000 –standardi kokonaisvaltaisena turvallisuuden hallintajärjestelmänä: Case Vacon Oyj

Kukkonen, Esa

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

ISO 28000 –standardi kokonaisvaltaisena turvallisuuden hallintajärjestelmänä: Case Vacon Oyj

Kukkonen, Esa
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Tammikuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Kukkonen, Esa

ISO 28000 –standardi kokonaisvaltaisena turvallisuuden hallintajärjestelmänä: Case Vacon Oyj

Vuosi 2014 Sivumäärä 62

Tässä laadullisessa tapaustutkimuksessa selvitetään ISO 28000 -standardin sovellettavuus alkuperäisestä toimitusketjun turvallisuuden hallintajärjestelmiin kohdistuvasta soveltamisalastaan laaja-alaiseksi, kokonaisvaltaiseksi yritysturvallisuuden hallintajärjestelmäksi. Kokonaisvaltaisella turvallisuuden hallintajärjestelmällä tarkoitetaan tässä tutkimuksessa järjestelmää, joka sisältää joukon systemaattisia ja koordinoituja toimintoja ja käytäntöjä, joiden avulla organisaatio pyrkii parhaalla mahdollisella tavalla hallitsemaan tähän kohdistuvia riskejä sekä niiden aiheuttamia mahdollisia uhkia ja seurauksia. Kaksiosaisessa tutkimuksessa arvioidaan standardia kokonaisvaltaisena turvallisuuden hallintajärjestelmänä sekä soveltuvuutta Vacon Oyj:n (jäljempänä ”Yritys”) käyttöön, turvallisuuden hallintajärjestelmän uudistamiseksi ja kehittämiseksi. Tutkimuksen teoreettinen viitekehys perustuu turvallisuuden hallintaa käsittelevään kirjallisuuteen ja tutkimuksen toteuttamisessa käytettyihin standardeihin ja standardinomaisiin viitekehyksiin.

Tutkimuksen ensimmäisessä vaiheessa tutkitaan ISO 28000 -standardin soveltuvuutta soveltamisalansa ulkopuolelle vertailuanalyysin, sisällönanalyysin ja asiantuntijahaastattelun keinoin. Teemoitteluun perustuvassa vertailuanalyysissä standardia verrataan muihin hallintajärjestelmiksi miellettyihin viitekehyksiin ja arvioidaan, täyttääkö se hallintajärjestelmille asetetut vaatimukset. Sisällönanalyysissä standardia tarkastellaan objektiivisesti, etsien standardin itsensä asettamia rajoitteita. Asiantuntijahaastattelussa analysoidaan johtamis- ja hallintajärjestelmiin perehtyneen laatupäällikön näkemystä standardin sovellettavuudesta.

Toisessa vaiheessa arvioidaan Yrityksen johtoryhmän (VEMT) ja laatupäällikön asiantuntijahaastatteluin, täyttääkö standardi Vacon Oyj:n turvallisuuden hallinnalle asettamat tarpeet ja vaatimukset. Tutkija esittää myös subjektiivisen näkemyksensä standardin sovellettavuudesta.

Tutkimuksen tuloksena todetaan, että ISO 28000 -standardia voidaan soveltaa soveltamisalastaan poikkeavaksi hallintajärjestelmäksi, sillä se sisältää hallintajärjestelmiltä vaadittavat elementit, eikä se itsessään rajoita soveltamisalasta poikkeamista. Tutkimuksessa todetaan myös, että ISO 28000 -standardi soveltuu kohdeorganisaation käyttöön, sillä se vastaa osittain jo käytössä olevia johtamisjärjestelmiä. Standardin todetaan vastaavan myös johtoryhmän asettamia tarpeita ja tahtotilaa turvallisuuden hallinnan periaatteille ja laajuudelle.

Asiasanat: Turvallisuuden hallinta, hallintajärjestelmä, ISO 28000, turvallisuusjohtaminen, standardi.

Laurea University of Applied Sciences
Leppävaara
Security Management Programme

Abstract

Kukkonen, Esa

ISO 28000 as a Corporate Security Management System: the Case of Vacon Oyj

Year 2014 Pages 62

The purpose of this research is to examine applicability of the ISO 28000 "Security Management Systems for the Supply Chain" -standard as a comprehensive framework of corporate security management system. In this research, the scope of corporate security management is defined as a system consisting of systematic and coordinated procedures and practices through which an organization optimally manages its risks, and the associated potential threats and impacts therefrom. The research has two sections and approaches to the ISO 28000-standard. The theoretical framework of the research is based on literature and security management standards and other management related frameworks being used in the research process.

In the first section the standard is being analysed and examined theoretically as a security management system. A comparative analysis, a content analysis and elite interview are being used as research methods. In the comparative analysis, based on thematising, the standard is being compared to other management system standards and frameworks to discover if the standard contains such elements and procedures that are essential for a management system. In the content analysis, the standard is objectively being analysed to disentangle the possible restrictions to the scope by the standard document. In the elite interview, Vacon Oyj's vice president in quality management, specialized in management systems, is being interviewed to assess the applicability of the standard.

In the second section the research analyses the applicability of the standard as a framework to further develop Vacon Oyj's corporate security management system. Vacon Executive Management Team (VEMT) and the vice president in quality are being interviewed to find out if the standard meets the needs and requirements of Vacon's security management principles. The researcher also states a subjective opinion of the applicability of the standard for the use of the Company.

In conclusion, the research states that the ISO 28000-standard can be applied as a comprehensive management system, as it contains all the needed elements of a management system and the standard document does not limit the deviation of the scope. The research also states that the standard can be applied to the Company, as it is partially consistent with the Vacon's existing management systems and it meets the needs and requirements for a corporate security management system, aligned by the VEMT.

Keywords: Corporate security, management system, ISO 28000, security management, standard.

Sisällys

1 Johdanto

Tämän laadullisen tutkimuksen tarkoituksena on tutkia kansainvälisen ISO 28000 *"Toimitusketjun turvallisuuden hallintajärjestelmät"* –standardin soveltuvuutta kokonaisvaltaiseksi turvallisuuden hallintajärjestelmäksi, työn tilaajan Vacon Oyj:n, jäljempänä "*Yritys*", käyttöön. Kokonaisvaltaisella turvallisuuden hallintajärjestelmällä tarkoitetaan tässä tutkimuksessa järjestelmää, joka sisältää joukon systemaattisia ja koordinoituja toimintoja ja käytäntöjä, joiden avulla organisaatio pyrkii parhaalla mahdollisella tavalla hallitsemaan tähän kohdistuvia riskejä sekä niiden aiheuttamia mahdollisia uhkia ja seurauksia (ISO 28000 2007, 10). Tutkimuksessa selvitetään ISO 28000 -standardin sovellettavuus alkuperäisestä toimitusketjuihin painottuvasta soveltamisalastaan laaja-alaiseksi, kokonaisvaltaiseksi yritysturvallisuuden hallintajärjestelmäksi. Tutkimus on kaksiosainen. Ensimmäisessä vaiheessa eritellään teoriapainotteisesti vertailuanalyysin keinoin turvallisuuden hallintaan liittyviä viitekehyksiä, turvallisuuden hallintajärjestelmältä vaadittavien, keskeisten elementtien ominaisuuksien määrittelemiseksi ja kuvaamiseksi. ISO 28000 -standardin soveltuvuutta kokonaisvaltaiseksi turvallisuuden hallintajärjestelmäksi arvioidaan vertaamalla standardin ominaisuuksia, hallintajärjestelmästandardien vertailuanalyysissä saatuun yleistykseen. Lisäksi ISO 28000 -standardia tutkitaan sisällönanalyysin keinoin mahdollisten soveltamisalaa koskevien rajoitteiden toteamiseksi sekä soveltuvuutta arvioidaan haastattelemalla johtamisjärjestelmiin perehtynyttä henkilöä.

Seuraavassa vaiheessa kartoitetaan Yrityksen johdon tahtotilaa ja päämääriä turvallisuuden hallinnan suhteen. Lisäksi kartoitetaan laatu- ja johtamisjärjestelmistä vastuussa olevan henkilön näkemyksiä käsiteltävän viitekehyksen soveltamisesta Yrityksen käyttöön laadunhallinnan ja johtamisen näkökulmasta. Yleistäen, tutkimuksen toisessa vaiheessa selvitetään Yrityksen halukkuus ja valmiudet täyttää hallintajärjestelmästandardin asettamat vaatimukset. Yrityksen asettamien linjauksien perusteella tutkija arvioi ISO 28000:n sovellettavuutta kohdeorganisaation käyttöön. Tutkimuksessa ei käsitellä tai kuvata Yrityksen turvallisuuden hallinnan lähtö- tai nykytilaa, sillä tutkimuksen toteuttamiseen on käytetty ainoastaan prosessin aikana tuotettua, kokonaan uuden järjestelmän rakentamisen kannalta oleellista tietoa, jolla ei ole yhteyttä jo olemassa olevien järjestelmien rakenteisiin ja toimintoihin.

Tutkimuksen toteuttaminen on kuvattu luvussa 2. Tutkimusstrategiaa havainnollistetaan luvussa 2.1 ja tutkimuksen suunnitelma sekä toteuttamiseen käytetyt menetelmät kuvataan luvuissa 2.2-2.2.5. Turvallisuuden hallinnan teoriaa käsitellään tutkimuksen viitekehyksen avaamiseksi luvussa 3. Tutkimuksessa käytettyjä turvallisuuden hallinnan viitekehyksiä ja niihin liittyvää valintaprosessia kuvataan alaluvuissa 3.1-3.1.6. Luku 3.2 alalukuineen on kokonaisuudessaan kuvaus vertailuanalyysistä johtopäätöksineen. ISO 28000 -standardin soveltuvuutta kokonaisvaltaiseksi hallintajärjestelmäksi arvioidaan teoriatasolla luvussa 4. Luvussa 5

kuvataan Yrityksen johtoryhmän ja laatupäällikön haastattelut kysymyksineen ja johtopäätöksineen. Tutkija esittää tutkimustuloksensa luvussa 6, jossa todetaan mahdollisuudet soveltaa standardia kokonaisvaltaiseksi yritysturvallisuuden hallintajärjestelmäksi sekä yleisluontoisesti että kohdeorganisaation käyttöön. Viimeisessä luvussa tutkija pohtii tutkimusprosessin kulkua ja haasteita sekä tutkimuksen johtopäätöksiin liittyviä rajoitteita ja yleistettävyyttä. Tutkija esittää myös tutkimusprosessin aikana ilmenneet tarpeet jatkotutkimukselle ja –kehittämistyölle.

1.1 Tutkimuksen tausta

Vacon Oyj on taajuusmuuttajia valmistava yritys, joka työllistää noin 1600 henkeä. Yrityksellä on tuotekehitystoimintaa Euroopassa, Aasiassa ja Pohjois-Amerikassa sekä noin 30 myyntiedustajaa ja 90 huoltoyhtiötä ympäri maailman. Yrityksen liikevaihto vuonna 2013 oli noin 403,0 miljoonaa euroa.

Yritys aloitti syksyllä 2013 AEO-sertifiointiin (Tullin valtuutettu taloudellinen toimija –status) tähtäävän turvallisuuden kehittämishankkeen. Työn edetessä hanketta koordinoinut työryhmä havaitsi, että turvallisuuden hallintaan ja johtamiseen liittyviä prosesseja, resursseja ja vastuita tulisi kehittää ja määritellä uudelleen. Sertifioinnin asettamien vaatimusten täyttämiseksi Yritys teki päätöksen uudistaa koko turvallisuuden hallintajärjestelmänsä.

AEO:n havaittiin hankkeen edetessä viittaavan ISO 28000 -standardiin, johon perustuen se on soveltamisalaltaan ISO 28000 –standardia osittain vastaava. Suunnittelutyön edetessä työryhmä havaitsi osan Yrityksen turvallisuuteen liittyvistä prosesseista olevan helposti sovellettavissa ISO-järjestelmien edellyttämään muotoon, joka synnytti tarpeen ja tahtotilan tutkimuksen suorittamiseksi.

1.2 Aikaisempi tutkimus

Suoraan tutkimusongelmaan vastaavaa aiempaa tutkimusta ei suoritetun tiedonhaun perusteella ole tehty tai sitä ei ole julkisesti saatavilla. Aihetta sivuaa yksi Venäjän kauttakulkuliikenteen turvallisuusriskejä ja ennaltaehkäisemistä käsittelevä tutkimus, jossa Liimatta (2011, 13) toteaa ISO 28000 -standardin soveltuvan eritoten yritysjohdon työkaluksi kokonaisturvallisuuden hallintaan. Johtopäätöksen tueksi Liimatta ei kuitenkaan esitä minkäänlaisia perusteluita vaan viittaa Laatukeskuksen vuonna 2010 järjestämään ISO 28000 -seminaariin, jonka aineistoa ei enää tämän tutkimuksen ajankohtana ollut saatavilla.

Tutkimuksen strategiaa mukailevia tutkimuksia löytyi useampia. Kunttu (2009) vertailee erilaisia turvallisuusjohtamiseen keskittyviä standardeja, mukaan lukien ISO 28000, mutta tutki-

muksessa tätä tarkastellaan ainoastaan sen alkuperäisen soveltamisalansa eli toimitusketjun näkökulmasta, eikä sen soveltuvuutta kokonaisvaltaiseksi turvallisuuden hallintajärjestelmäksi arvioida.

Stenberg (2014) tutkii työssään Maanpuolustuskorkeakoulun turvallisuusjohtamisjärjestelmää. Organisaation turvallisuusjohtamisjärjestelmän ja sen ominaisuuksien kuvaamiseksi Stenberg laatii mallin toimialasta ja kohdeorganisaatiosta riippumattomasta johtamisjärjestelmästä sisältövaatimuksineen. Tutkimuksessa ei käsitellä ISO 28000 –standardia. Tässä tutkimuksessa mukaillaan Stenbergin tutkimusstrategiaa, turvallisuuden hallinnan keskeisten elementtien ja piirteiden jäsentämiseksi ja ISO 28000 –standardin soveltuvuuden arvioimiseksi. Stenbergin tutkimukseen työssä ei kuitenkaan haluttu suoraan tukeutua, sillä ammattikorkeakoulun opinnäytetyötä ei pidetty riittävän luotettavana lähteenä. Myös tutkimuksessa tarkasteltavat viitekehykset eroavat Stenbergin vastaavista.

1.3 Tutkimuksen tavoitteet ja rajaus

Tutkimus käsittelee tutkimusongelmia ainoastaan teoreettisella tasolla. Tutkimus ei ota kantaa ISO 28000 -standardin käytännön sovellutukseen yleisesti tai kohdeorganisaation käyttöön. Tutkimuksen tavoitteena on laatia teoriaan pohjautuva selvitys, soveltuisiko ISO 28000 -standardi kokonaisvaltaiseksi turvallisuuden hallintajärjestelmäksi ja sekä kohdeorganisaation käyttöön.

Tutkimuskysymyksiksi on asetettu:

1. Soveltuuko ISO 28000 -standardi organisaation kokonaisvaltaisen turvallisuuden hallintajärjestelmän viitekehykseksi?
2. Vastaako ISO 28000 –standardiin perustuen mahdollisesti rakennettava järjestelmä organisaation tarpeita?

Tutkimuksen teoreettinen viitekehys on rajattu aihetta käsittelevään kirjallisuuteen ja standardeihin sekä standardinomaisiin kehyksiin. Tutkimuksesta on jätetty pois muun muassa lainsäädännön tarkastelu, koska a) lakien ja asetusten katsotaan olevan sisällöltään liian laveita asettamaan selkeitä vaatimuksia turvallisuuden johtamiselle ja b) kohdeorganisaatio harjoittaa liiketoimintaa useassa maanosassa. Vaikka lainsäädännön tarkastelu viitekehyksen kannalta ei olisikaan epäolennaista, tutkimuksessa halutaan kuitenkin pohjautua ainoastaan kansainvälisiin viitekehyksiin ja välttää täten kansainvälisellä tasolla poikkeavien kansallisten lainsäädäntöjen mahdollisesti aiheuttamat konfliktit.

Tutkimuksessa mallinnetusta turvallisuusjohtamisen yleistyksestä ei pyritä luomaan universaalia, jokaiseen tapaukseen soveltuvaa ja aukotonta uutta hallintajärjestelmästandardia. Yleistyksen tarkoituksena on toimia vertailukohtana tutkimuksen keskiössä olevalle ISO 28000 -standardille. Tutkimuksessa tuotetun tiedon soveltuvuutta muihin tapauksiin arvioidaan pohdintaosiossa, luvussa 7.

1.4 Keskeiset käsitteet

Turvallisuuden hallintajärjestelmä. Turvallisuuden hallinnalla tarkoitetaan joukkoa systemaattisia ja koordinoituja toimintoja ja käytäntöjä, joiden avulla organisaatio pyrkii parhaalla mahdollisella tavalla hallitsemaan tähän kohdistuvia riskejä sekä niiden aiheuttamia mahdollisia uhkia ja seurauksia. (ISO 28000 2007, 10.)

Johtamisjärjestelmä. Johtamisjärjestelmällä tarkoitetaan järjestelmää, jonka tarkoituksena on saavuttaa politiikan ja tavoitteiden asettamat määrittelyt. Organisaation johtamisjärjestelmä voi sisältää erilaisia johtamisjärjestelmiä, kuten laadunhallintajärjestelmä, taloushallintajärjestelmä ja ympäristönhallintajärjestelmä. (ISO 9000 2005, 24.)

Standardi. Standardilla tarkoitetaan jotakin linjausta, jolle on ominaista yhteinen menettelytapa toistuvaan toimintaan. Standardit ovat luonteeltaan suosituksia, mutta viranomaiset saattavat edellyttää niiden käyttöä. Standardi on kirjallinen julkaisu ja standardisoinnista huolehtivan viranomaisen, järjestön tai muun tunnustetun elimen hyväksymä. (Suomen standardisoimisliitto 2014a.) Standardin alakäsitteellä, **hallintajärjestelmästandardilla** tarkoitetaan standardia, jolla tähdätään parempaan toimintaan – laadukkaat ja tehokkaat prosessit, turvalliset toimintatavat, hyvä ympäristöasioiden hoito sekä riskien vähentäminen. Tuloksena ovat tyytyväisemmät asiakkaat, työntekijät ja muut sidosryhmät. (Suomen standardisoimisliitto 2014b.)

2 Kvalitatiivisen tapaustutkimuksen toteuttaminen

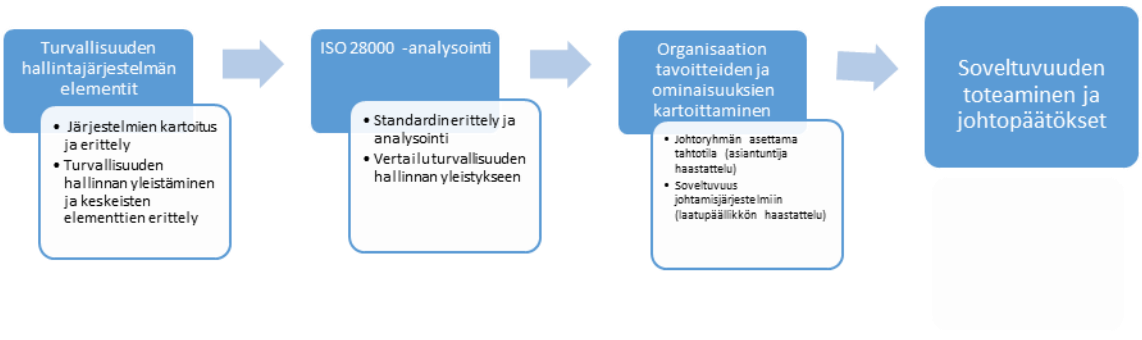
Tutkimuksen tulokulmaksi on valittu laadullinen tapaustutkimus, koska Bambergin, Jokisen ja Laineen (2007, 10) mukaan juuri tapaustutkimukselle on ominaista selvittää jotakin ilmiötä, joka ei ole entuudestaan tiedossa, mutta joka kaipaa lisävalaisua. Lisäksi tapaustutkimukseen pohjautuva vertaileva tutkimus toimii hyvin, kun analysoitavien tapausten (hallintajärjestelmä viitekehykset) määrä on suhteellisen pieni (Bamberg ym. 2007, 77). Tapaustutkimus vastaa parhaiten tutkimuksen ongelmiin, selvittäen miten ja miksi ISO 28000 -standardi soveltuu kokonaisvaltaiseksi turvallisuuden hallinnan viitekehykseksi ja kohdeorganisaation käyttöön.

Tapaustutkimuksen tuloksia voidaan yleistää joko kattamaan tapausta laajempaa kokonaisuutta tai yleistäminen voidaan luoda tapauksen sisään (Bamberg ym. 2007, 27). Tutkimuksessa on tavoiteltu jälkimmäistä vaihtoehtoa, sillä yleistyksen tarkoituksena on palvella nimenomaan tässä tutkimuksessa käsiteltävän tapauksen viitekehyksenä.

Tutkimuksen lähestymistapa täyttää myös Grounded Theory -menetelmän tai tyylisuunnan ominaispiirteet. Tyylisuunnassa tutkimuksen perusväittämiä ei muotoilla aiemman tutkimuksen tai teorian perusteella, vaan tutkimuksessa käytetyn aineiston perusteella. Teoria ja viitekehys syntyvät tutkijan ja aineiston vuorovaikutuksessa, peilaten tutkijan esiymmärrykseen tutkittavasta ilmiöstä, toimien luokittelun eli kategorioinnin kokoajana ja perusteluna. (Anttila 2006, 376.)

2.1 Tutkimusstrategia ja -suunnittelma

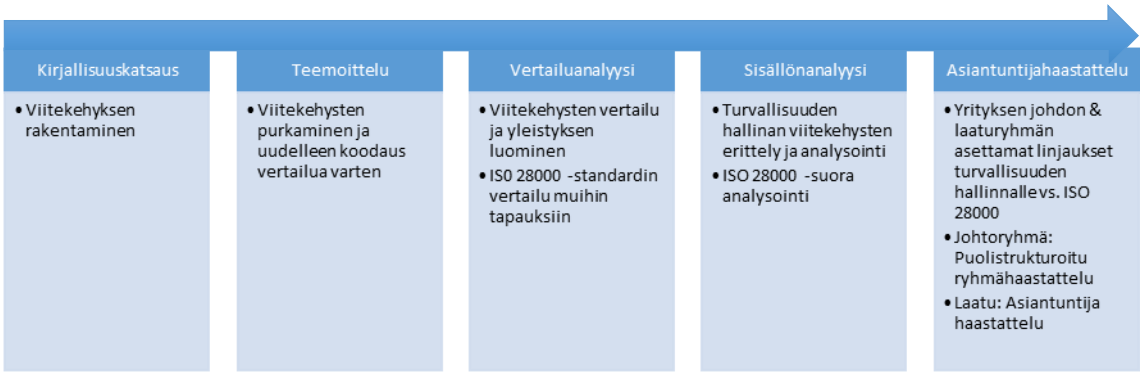
Tutkimuksen pohjana on tutkijan laatima tutkimusstrategia, jossa tutkimus jaetaan loogisiin ja kronologisiin vaiheisiin. Tutkimuksen ensimmäisessä vaiheessa rakennetaan tutkimuksen viitekehys kartoittamalla, valitsemalla ja erittelemällä turvallisuutta ja hallintajärjestelmiä käsitteleviä standardeja ja standardinomaisia viitekehyksiä. Toisessa vaiheessa eritellään ISO 28000 -standardia, jotta sitä voidaan verrata hallintajärjestelmien yleistykseen sekä arvioida sen sovellettavuutta muista näkökulmista. Kolmannessa vaiheessa kartoitetaan Yrityksen tahtotilaa turvallisuuden hallinnan ja sen periaatteiden selvittämiseksi ja ISO 28000 -standardin soveltumiseksi kohdeorganisaatioon. Viimeisessä vaiheessa tutkija tekee yhteenvedon aiempien vaiheiden tuloksista ja esittää johtopäätöksensä. Tutkimusstrategiaa havainnollistetaan kuvassa 1.



Kuvio 1 Tutkimusstrategia

Tutkimusstrategian toteuttamiseksi on laadittu yksityiskohtaisempi tutkimussuunnitelma, jossa määritellään alustavat metodologiset valinnat tutkimuksen suorittamiseksi. Tutkimuksen luotettavuutta on pyritty parantamaan triangulaation keinoin. Tutkimuksen pääkysymystä kä-

siteltiin kolmella metodilla. ISO 28000 -standardia tutkitaan objektiivisesti sisällönanalyysin keinoin, asettaisiko standardi itsessään rajoitteita alkuperäisestä soveltamisalasta poikkeamiseen. Toiseksi standardia käsitellään analyyttisesti vertailemalla sitä teemoittelun ja vertailun keinoin eriteltyihin turvallisuuden hallinnan oleellisiin elementteihin ja soveltamisalaltaan hallintajärjestelmiksi miellettyihin viitekehyksiin. Kolmanneksi standardin soveltuvuutta arvioidaan haastattelemalla johtamis- ja hallintajärjestelmiin perehtynyttä henkilöä, jolta pyydettiin subjektiivinen mielipide standardin soveltuvuudesta kokonaisvaltaiseksi hallintajärjestelmäksi. Tutkimussuunnitelma on kuvattu kuviossa 2. Tutkimuksessa käytettyjä tutkimusmenetelmiä käsitellään tarkemmin luvuissa 2.2-2.2.5.



Kuvio 2 Tutkimussuunnitelma

2.2 Tutkimusmenetelmät

Seuraavissa alaluvuissa kuvataan tutkimukseen suunnitellut tutkimusmenetelmät sekä niiden käyttökohteet. Tutkimusmenetelmät valittiin tutkimusmenetelmäoppaiden (mm. Anttila 2006; Hirsjärvi, Remes & Sajavaara 2009) perusteella, joita tutkimalla pyrittiin löytämään kuhunkin tutkimuskohteeseen ja -ongelmaan parhaiten soveltuva menetelmät. Tutkimusmenetelmien soveltuvuutta tutkittavaan aiheeseen arvioidaan pohdintaosiossa, luvussa 7.

2.2.1 Kirjallisuuskatsaus ja tiedonhaku

Tutkimuksen teoreettisen viitekehyksen laatimiseksi, tietoperustan rakentamiseksi sekä keskeisten käsitteiden määrittelemiseksi on laadittu kirjallisuuskatsaus. Hirsjärven ym. (2009, 109) mukaan tutkimusaihetta käsittelevään kirjallisuuteen perehtyminen ohjaa tutkimusstrategian suunnittelussa, tutkimuskysymysten asettelussa sekä metodologisissa valinnoissa. Katsauksessa on hyödynnetty sekä kansallisia että ulkomaisia kirjallisia ja sähköisiä lähteitä.

Elektroniseen tiedonhakuun on käytetty ammattikorkeakoulujen opinnäytetöistä koostuvaa Theseus-julkaisuarkistoa sekä Googlen vapaasanahakua että Google Scholar-hakua. Hakukoneeksi on valittu Google, sillä se on hakuroboteista käytetyin, ja sillä on laajin tietokanta (Hirsjärvi ym. 2010,90). Hakusanoina on käytetty seuraavia termejä: ”turvallisuuden hallinta”, ”turvallisuuden hallintajärjestelmä”, ”security management standard”, ”security management framework” ”turvallisuusjohtaminen”, ”yritysturvallisuus”, ”corporate security”, ”ISO 2800*” ja ”turvallisuusstandardit” sekä edellä mainittujen eri variaatioita.

Kirjallisuuskatsauksessa on tarkasteltu keskiössä olevien standarditekstien lisäksi turvallisuuden hallintaa käsittelevää kirjallisuutta. Tutkimuksen teoreettisen viitekehyksen tukemiseksi on valittu sekä kansallisesti että kansainvälisesti turvallisuuden hallintaa käsitteleviä teoksia. Kirjallisuuskatsauksen tärkeimpiä teoksia ovat Pertti Kerkon, 2001, ”Turvallisuusjohtaminen” ja Leppäsen, 2006, ”Yritysturvallisuus käytännössä”. Teoksissa kuvataan turvallisuuden hallinnan periaatteita, tavoitteita ja keskeistä sisältöä, joita tutkija pyrkii tässä tutkimuksessa jäsentämään. Kansainvälisestä näkökulmasta turvallisuusjohtamiseen on tarkasteltu Halibozekin ja Kovacichin vuonna 2003 julkaisemaa teosta ” The manager’s handbook for corporate security: establishing and managing a successful assets protection program”. Kirjallisuuskatsauksessa on paneuduttu myös korkeakoulujen opinnäytetöihin ja yhteen väitöskirjaan (mm. Kuntu 2006 ja Levä 2003) sekä erilaisiin tutkimusmenetelmä oppaisiin (mm. Hirsjärvi 2009 ja Anttila 2006) tutkimusstrategian, -suunnitelman ja -menetelmien valitsemiseksi.

2.2.2 Sisällönanalyysi

Sisällönanalyysillä tarkoitetaan tekstianalyysiä, jossa tarkastellaan tekstimuotoisia tai tekstimuotoon muutettuja aineistoja eritellen, yhtäläisyyksiä ja eroja etsien sekä tiivistäen. Sisällönanalyysin keinoin pyritään muodostamaan tutkittavasta ilmiöstä kuvaus, joka kytkee tulokset ilmiön laajempaan kontekstiin ja muihin olennaisiin tutkimustuloksiin. (Saaranen-Kauppinen & Puusniekka 2006.) Sisällönanalyysin haasteita osana tätä tutkimusta käsitellään tutkimuksen pohdintaosiossa, luvussa 7.

Tutkimuksessa on sovellettu laadullista ja aineistolähtöistä sisällönanalyysiä sekä viitekehyksen rakentamisessa käytetyn aineiston erittelyssä että ISO 28000 –standardin suorassa analysoinnissa. Ensisijaisesti standardista on etsitty ilmaisuja, jotka viestivät kielteisesti poikkeamasta ja soveltamasta standardin alkuperäistä soveltamisalaa. Lisäksi tekstiaineistosta on etsitty myös ehdottomia ilmaisuja, jotka joko a) linkittäisivät standardin absoluuttisesti toimitusketjujen turvallisuuteen tai b) määrittelisivät, että standardi ei täytä hallintajärjestelmille asetettuja vaatimuksia.

2.2.3 Teemoittelu

Laadullisessa tutkimuksessa analyyttinen kehys ja aineisto tarkentuvat tutkimuksen edetessä. Aluksi valitaan tutkimuksessa tarkasteltavat tapaukset, joiden avulla määritellään, minkälaisia käsitteitä ja luokkia itse tarkastelussa tarvitaan. Lopulta kuitenkin muodostuu tarkempi analyyttinen kehys, joka kuitenkin pohjautuu nimenomaan tutkittavien tapausten erityspiirteisiin. (Bamberg ym. 2007, 88.) Kehyksen luomiseksi, tarvittavat luokat ja käsitteet muodostettiin teemoittelemalla.

Teemoittelulla pyritään muodostamaan keskeisiä aiheita, jotka ovat esiintyvät tarkasteltavissa aineistoissa (Saaranen-Kauppinen & Puusniekka 2006). Aineistoista voidaan muodostaa teemoja esimerkiksi koodaamalla. Koodauksessa tutkija etsii ja merkitsee aineistoista tutkimuksen kannalta oleellisia asioita pyrkimyksenään selkeyttää aineiston sisältöä. Koodaamalla voidaan siis selvittää, mitä tutkimusaiheeseen liittyvää aineisto sisältää (Saaranen-Kauppinen & Puusniekka 2006).

Käsiteltävistä viitekehyksistä on pyritty löytämään sisällönanalyysillä keskeinen sisältö, turvallisuuden hallinnalle asetetut vaatimukset, ja koodaamaan ne valmiiksi hahmoteltujen kategorioiden mukaan (kuten ”Politiikka”, ”Johdon sitoutuminen” jne.). Aineistoista on etsitty ilmaisuja, jotka joko vaatisivat tai ohjeistaisivat viitekehyksen implementoijaa jonkin menettelyn toteuttamisessa. Koodauksessa keskeisiä ilmaisuja olivat ”yrityksen tulee/tulisi luoda” ja ”yrityksen on/olisi luotava” –muodossa esitetyt asiakokonaisuudet sekä näihin rinnastettavat ilmaisut. Poikkeuksena joukossa esiintyy AEO, joka ei määrittele tai velvoita yksityiskohtaisia menettelyjä. Sen sijaan AEO-dokumentaatio esittää hyväksynnän kannalta oleellisesti vaatimukset kysyen tai ehdottaen, esimerkiksi ”Onko olemassa dokumentoituja turvakäytäntöjä?” (Euroopan komissio 2012, 62).

Koodauksen avulla tarkastellut aineistot on voitu purkaa ja järjestää uudelleen muotoon, jossa kaikki viitekehykset ovat keskenään vertailukelpoisia. Luodut teemat edustavat yhden tai useamman viitekehyksen asettamaa hallintajärjestelmän vaatimusta tai elementtiä. Selkeyden vuoksi teemojen nimittämisessä on pyritty mukailemaan ISO –standardien termistöä ja rakennetta.

Suoraan tutkimuskysymystä käsitteleviä julkaisuja ei löytynyt. Suoritettu tiedonhaku vahvistaa edelleen tutkimuksen mielekkyyttä ja sen mahdollisuutta tuottaa uutta tietoa. Tiedonhaku on vahvistanut osaltaan myös tutkimusstrategian toimivuutta, sillä vastaavin menettelyin on toteutettu useita nimenomaan turvallisuusjohtamiseen ja –hallintaan liittyviä tutkimuksia.

2.2.4 Haastattelut

Tutkimuksen toisena tavoitteena on pyritty selvittämään ISO 28000 –standardin mahdollisuutta täyttää kohdeorganisaation johdon asettamat tarpeet sekä tavoitteet turvallisuuden hallinnan suhteen. Kohdeorganisaation toivomuksesta työ suoritetaan niin sanotusti puhtaalta pöydältä, joka tarkoittaa käytännössä sitä, että selvitystyössä ei ole tukeuduttu dokumentaatioon. Hirsjärven ym. (1997, 205) mukaan haastattelu tiedonkeruumenetelmänä on erityisesti perusteltua silloin, kun ihminen (tässä tutkimuksessa myös ryhmä) halutaan nähdä subjektina. Tässä tutkimuksessa haastateltavat ovat merkityksiä luova ja aktiivinen osapuoli. Tarvittava aineisto on kerätty haastattelemalla Yrityksen johtoryhmää sekä henkilöä, joka vastaa Yrityksen johtamis- ja toiminnanohjausjärjestelmien ylläpidosta ja kehittämisestä.

Johtoryhmän haastattelun osalta tiedonkeruumenetelmäksi on valittu puolistrukturoitu ryhmähaastattelu. Puolistrukturoidulla rakenteella on pyritty luomaan mahdollisimman selkeä, asiapainotteinen ja tutkimuskysymyksiin vastaava haastattelu, joka jättäisi kuitenkin tilaa vapaalle keskustelulle ja ideoinnille. Ryhmähaastattelulle on ominaista, että tutkimuksessa ei välttämättä olla lainkaan kiinnostuneita yksittäisten ihmisten mielipiteistä ja ajatuksista vaan kiinnostuksen kohteena on ennen kaikkea ryhmän kollektiivinen näkemys (Hirsjärvi & Hurme 2009, 61). Haastattelu päädyttiin pitämään ryhmässä, koska näillä keinoin pyrittiin välttämään jyrkästi eriäviä mielipiteitä, jotka olisivat mahdollisesti vesittäneet johtoryhmän kollektiivisen vision turvallisuustyön tavoitteista ja päämääristä. Lisäksi, itse haastattelutilaisuudella katsottiin olevan tärkeä rooli johdon sitouttamisessa turvallisuustyöhön - Yrityksen johto saatiin mukaan jo järjestelmän visiointi- ja suunnitteluvaiheessa.

Johtoryhmän lisäksi tutkimuksessa on haastateltu asiantuntijahaastatteluna Yrityksen laatupäällikköä ISO 28000 –standardin soveltuvuuden arvioimiseksi Yrityksen käyttöön. Asiantuntijahaastattelulla (elite interviewing) tarkoitetaan haastattelua, jossa haastateltavat on valittu tarkoin juuri tutkittavaa ilmiötä varten asiantuntemuksensa johdosta. Haastateltavat voivat asemansa puolesta antaa tietoa jonkin ilmiön laajoista kysymyksistä tai yksittäisistä teknisistä yksityiskohdista. Haastattelulla pyritään kokoamaan asiantuntijan hallussa oleva erikoistietämys. (Anttila 2006, 198-199.) Tutkimuksessa on päädytty haastattelemaan kohdeorganisaation laatupäällikköä, sillä hänellä katsottiin olevan parhain mahdollinen tietämys Yrityksen laatu- ja johtamisjärjestelmistä sekä näiden järjestelmien yleisistä edellytyksistä.

Asiantuntijahaastattelun runkona käytettiin ISO 28000 -standardista eriteltyä vaatimuslistaa (ks. 3.1.3). Haastateltavaa pyydettiin vertaamaan standardin asettamia vaatimuksia Yrityksen nykyiseen laatu- ja johtamisjärjestelmään ja arvioimaan olisiko kyseinen vaatimus toteutettavissa. Laatupäällikköä pyydettiin myös arvioimaan ISO 28000 -standardia kokonaisvaltaisena hallintajärjestelmänä, sisältäisikö se kaikki johtamisjärjestelmille olennaiset elementit ja

piirteet. Kysymyksellä tavoiteltiin asiantuntijan näkemystä tutkimuksen pääkysymykseen, joko vahvistamaan tai haastamaan tutkijan tekemät, teoriaan pohjautuvat johtopäätökset.

Haastattelujen aineistot on purettu suoraan äänitteistä litteroimatta. Hirsjärven ym. (2009, 138) mukaan päätelmien tekeminen suoraan tallenteista on mahdollista silloin, kun haastateltavia on ollut vain muutamia ja haastattelut ovat olleet ajallisesti lyhyitä. Analysoinnin tulokulmaksi on valittu lähestymistapa, jossa haastattelija ei tee tulkintoja, vaan haastateltavat itse huomaavat merkityksiä ja tekevät päätelmiä asiayhteyksistä, joita eivät ole aiemmin tulleet huomanneeksi (Hirsjärvi & Hurme 2009, 137). Analysointi alkoi jo itse haastatteluvaiheessa, ja haastattelutilaisuuksilla itsessään oli osapuolista riippuen eri tavoitteet ja päämäärät. Tutkijan tavoitteena oli selvittää, soveltuisiko ISO 28000 –standardi Yrityksen turvallisuuden hallintajärjestelmän rungoksi. Sen sijaan Yrityksen edustajille haastattelu oli enemmänkin aivoriihi, jonka tuloksena syntyi uusia linjauksia turvallisuuden hallinnan toteuttamiseen. Koska aikaisempaa dataa asian suhteen ei ollut saatavilla, tutkimuksen kannalta haastattelun tuloksena syntyneet linjaukset olivat tärkeitä. Haastattelujen kysymyksiä ja analysoitua sisältöä eritellään tarkemmin luvuissa 4.1 ja 4.2.

2.2.5 Vertailuanalyysi

Tapausten vertailu on olennainen osa tapaustutkimusta (Bamberg ym. 2007, 74). Vertailuanalyysin keinoin on pyritty luomaan yksittäisten tapausten ominaisuuksista rinnakkainasetteluja, joiden konflikteista on johdettu teemoja - turvallisuuden hallinnalle keskeisiä elementtejä. Viitekehysten (tapausten) vertailu on aloitettu jo aineiston uudelleen koodaamisvaiheessa, jossa tapausten sopivuutta arvioitiin muihin samoihin kategorioihin (teemoihin) koodattujen tapausten kanssa.

3 Turvallisuuden hallinta

Tarve turvallisuuden hallinnalle on ollut olemassa niin kauan kuin jokin taho on tavoitellut toisen omistamaa voimavaraa, tämän olematta halukas siitä luopumaan tai kyseiseen voimavaraan on kohdistunut jokin muu ulkopuolinen uhka. Turvallisuuden hallinnan voidaan katsoa lähtevän yrityksen omistajastrategiasta. Yritys on velvoitettu palvelemaan omistajiensa intressejä sekä suojaamaan liiketoiminnan kilpailukyvyn. Hallinnalle vaatimuksia asettavat myös ulkoiset tekijät: Lait velvoittavat yrityksen takaamaan työntekijöilleen ja asiakkailleen turvallisen työympäristön sekä asiakkaat ja vakuutusyhtiöt vaativat yhteistyökumppaneiltaan erinäisiä turvallisuuskontrolleja. (Halibozek & Kovacich 2003, 49;65.)

Turvallisuuden hallinnasta käytetään useasti myös termiä turvallisuuden johtaminen (muun muassa KATAKRI). Kumpikaan termi ei ole täysin vakiintunut ja niiden välisiä eroavuuksia on

täten vaikea eritellä. Kerkon (2001, 22-23) mukaan on kuitenkin epäolennaista, mitä termiä järjestelmästä käytetään, sillä olennaisinta on sisältö: tarvittavia elementtejä ovat järjestelmäpiirteet, johtamispiirteet ja laatujärjestelmäpiirteet. Kerko jäsentää hallintajärjestelmän tietyksi kokonaisuudeksi, joka muodostuu ohjedokumenteista, sisäisistä turvallisuusoppaista, koulutukseen ja tiedotukseen liittyvistä multimediavalmisteista, turvamerkintätauluista ja muista työpaikoilla säilytettävistä turvallisuusmenettelyjä, lainsäädäntöä ynnä muuta koskevista julkaisuista, joista jokin taho selkeästi vastaa. (Kerko 2001, 23). Levä (2003, 38) esittää väitöskirjassaan, että turvallisuuden johtamisjärjestelmän keskeisimpänä tarkoituksena on varmistaa, että ennaltaehkäisevät toimenpiteet onnettomuuksilta suojautumiseksi ovat olemassa ja ne ovat toimivia. Järjestelmä sisältää ylätasolla neljä elementtiä: turvallisuustavoitteet, järjestelmä näiden tavoitteiden saavuttamiseksi, toimintaa koskevat vaatimukset sekä niiden seurantamenettelyt.

3.1 Turvallisuutta ja hallintajärjestelmiä ohjaavia viitekehyksiä

Turvallisuudelta ja hallintajärjestelmiltä vaadittavien menettelyiden yhdenmukaistamiseksi, standardisoimiseksi ja selkeyttämiseksi on luotu useita viitekehyksiä. Seuraavissa alaluvuissa esitellään turvallisuuden hallintaan ja yleisesti hallintajärjestelmiin painottuvia standardeja, sekä perustellaan, miksi kyseiset viitekehykset on valittu osaksi vertailua. Tutkimuksessa tavoitellun ”turvallisuuden hallinnan yleistyksen” luomiseksi, käsiteltäviä standardeja eritellään tarkemmin luvuissa 3.2.1-3.2.16 ja 3.3.

3.1.1 ISO 27001

Tietoturvallisuutta käsittelevä kansainvälinen standardi ISO/IEC 27001:2005 *”Informaatioteknologia. Turvallisuus. Hallintajärjestelmät. Vaatimukset.”* määrittelee vaatimukset, jotka koskevat dokumentoidun tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, käyttämistä, valvontaa, katselmointia, ylläpitoa ja parantamista. Vaatimuksissa huomioidaan myös yleiset liiketoimintariskit. Standardi on sovellettavissa kaikenlaisiin organisaatioihin. (ISO 27001 2005, 10.)

Standardi painottaa kyseessä olevan nimenomaan tietoturvallisuuden hallintajärjestelmä, yleisen yritysturvallisuus- ja johtamisjärjestelmän sijasta. Vahvan rajauksensa johdosta se määrittelee tietoturvallisuuden hallintajärjestelmän täysin omaksi kokonaisuudekseen. Sekä sisältönsä että rakenteensa osilta ISO 27001 –standardissa on kuitenkin erittäin paljon yhtymäkohtia etenkin laadunhallintaa käsittelevän ISO 9001 –standardin ja ympäristönhallintaa käsittelevän 14001-standardin kanssa, joita yleisesti sovelletaan yritysten johtamisen kulmakiviksi. (ks. 3.2.1-3.2.16.)

Standardi on valittu tarkasteluun, koska se käsittelee tutkimuksen kannalta oleellisen tekijän, hallintajärjestelmän, suunnittelua, toteuttamista ja ylläpitoa. Soveltamisalansa puitteissa ISO 27001vastaa pitkälti rakenteeltaan tutkimuksen kohteena olevaa ISO 28000 –standardia. Se käsittelee hallintajärjestelmää sen kaikkine elementteineen, kuitenkin rajattuna tiettyyn toimintoon tai toimintojoukkoon.

3.1.2 KATAKRI

Kansallinen turvallisuudenauditointikriteeristö KATAKRI on kansallisten viranomaisten käyttöön tai viranomaisten lukuun toimiville auditoijille kehitetty, tietoturvallisuuteen rajoittuva auditointityöväline. Auditointikriteeristön tarkoituksena on määritellä vaatimukset ja suojaustasot valtionhallinnon tietoturvallisuusasetuksen alaisten tietojen (käyttö rajoitettu, luottamuksellinen, salainen, kuitenkin pl. erittäin salainen) suojaamiseksi. Kriteeristöllä on myös sekundäärikäyttöä yritysten omaehtoisen turvallisuustoiminnan viitekehyksenä. (Puolustusministeriö 2011, 3-6; 124.)

KATAKRI ei määrittele turvallisuuden hallintaa tai turvallisuuden johtamista yksiselitteisesti. Kuitenkin, mikäli KATAKRI:n hallinnollisen turvallisuuden osa-aluetta (A100-A900) tarkastellaan kokonaisuutena, voidaan turvallisuuden hallinnan todeta sisältävän seuraavia elementtejä:

- turvallisuuspolitiikka ja toiminnan periaatteet tavoitteineen ja määritelmineen,
- organisaatio ja vastuut
- turvallisuuden toimintaohjelma ja ennaltaehkäisevien toimenpiteiden suunnittelu
- dokumentaatio ja sen hallinta
- turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen
- raportointi ja johdon katselmukset (jatkuva parantaminen).

KATAKRI:n hallinnollisen turvallisuuden osa-alueen muodostama turvallisuusjohtamisen kokonaisuus mukailee laajasti ISO-standardeissa käytettyä rakennetta. Viitekehyksenä KATAKRI on kuitenkin erilainen, sillä se asettaa ISO-standardeista poiketen tarkkoja ja ehdottomia vaatimuksia (pois lukien elinkeinoelämän suositukset) turvallisuusmenettelyjen toteuttamiseksi. KATAKRI on valittu tarkasteluun kokonaisvaltaisuudensa takia. Lisäksi tarkastelun kannalta eduksi on katsottu KATAKRI:ssa esiintyvät viittaukset IEC/ISO 27002-standardiin. KATAKRI:a eritellään tarkemmin luvuissa 3.2.1-3.2.16.

3.1.3 ISO 28000

ISO 28000 -standardi on tutkimuksen keskiössä. Kansainvälinen SFS-ISO 28000:2007 *"Toimitusketjun turvallisuuden hallintajärjestelmät"* -standardi määrittelee vaatimukset turvallisuuden hallintajärjestelmälle, mukaan lukien ne näkökohdat, jotka ovat kriittisiä toimitusketjujen turvallisuuden kannalta. Standardi on kehitetty vastaamaan teollisuuden vaatimuksia, ja sen perimmäisenä tarkoituksena on parantaa toimitusketjun turvallisuutta. (ISO 28000 2007, 6-10.)

Standardin avulla organisaation on mahdollista vakiinnuttaa, ylläpitää ja kehittää turvallisuuden hallintajärjestelmää, varmistaa vaatimustenmukaisuus turvallisuuden hallintapolitiikalla, hakea sertifiointia turvallisuuden hallintajärjestelmälle sekä todeta ja ilmoittaa toimivansa ISO 28000 –standardin mukaisesti. Standardi on sovellettavissa yrityskoosta ja riippumatta roolista toimitusketjussa. (ISO 28000 2007, 10.) Standardia eritellään tarkemmin luvuissa 3.2.1-3.2.16.

3.1.4 OHSAS 18001

OHSAS 18001, "Työterveys- ja työturvallisuusjohtamisjärjestelmät. Vaatimukset", määrittelee vaatimukset työterveyden ja työturvallisuuden (TTT) johtamisjärjestelmälle sekä esittää organisaatiolle tehokkaan TTT-järjestelmän rakenneosat. OHSAS-standardin yleinen tavoite on tukea ja edistää hyviä työterveys- ja työturvallisuuskäytänteitä tasapainossa sosiaalis-taloudellisten tarpeiden kanssa. Standardi on sovellettavissa kaikenkokoisiin ja -tyyppisiin organisaatioihin. (OHSAS 18001 2007, 10.)

OHSAS-standardi noudattaa riskiperusteista lähestymistapaa. TTT-järjestelmän tarkoituksena on poistaa tai minimoida organisaation toiminnasta henkilöstölle tai muille sidosryhmille mahdollisesti aiheutuvat TTT-vaarat (OHSAS 18001 2007, 14). Järjestelmä tai sen osia voidaan integroida osaksi muita johtamisjärjestelmiä, jota edesauttaa standardin osittainen vastaavuus ISO 9001 ja ISO 14001-standardien kanssa (OHSAS 18001 2007, 10). OHSAS-standardi on valittu tarkasteluun puhtaasti soveltamisalastaan johtuen. Kuten otsikointikin esittää, kyseessä on turvallisuutta käsittelevä johtamisjärjestelmästandardi, joka sisältää kaikki hallinta- ja/tai johtamisjärjestelmälle oleelliset elementit.

3.1.5 AEO – Authorized Economic Operator

AEO, englanniksi Authorized Economic Operator eli valtuutettu taloudellinen toimija, on Maailman tullijärjestön WCO:n kehittämä, Euroopan unionin tulliviranomaisten turvallisuusohjelma. Kunkin jäsenmaan tulliviranomainen voi myöntää yhteisön alueella toimivalle yritykselle

tullausta ja turvallisuutta koskevan todistuksen, mikäli viranomaisen arvioinnin mukaan yritys on vakavarainen, ja se täyttää tullausta ja turvallisuutta koskevat vaatimukset. Vastapainoksi yritys hyötyy muun muassa tullilupien nopeutetusta myöntämisestä sekä toimitusketjun turvallisuuden paranemisesta. (Tulli 2014.)

AEO-asemaa hakevan yrityksen on täytettävä Euroopan komission asettamat ja jäsenvaltion tulliviranomaisen soveltamat turvallisuusvaatimukset. Vaikka viitekehyksen pääpaino on toimitusketjujen turvallisuudessa, käsittää se kattavasti kaikki yritysturvallisuuden osa-alueet, pois lukien työterveyttä ja –turvallisuutta koskevat menettelyt. Kaiken perustana AEO:ssa painotetaan turvallisuusjohtamista. Tullihallituksen (2008, 3-6), nykyisen Tullin, mukaan yrityksellä tulee olla muun muassa turvallisuuspolitiikka, nimetyt turvallisuudesta vastaavat henkilöt, menettelyt turvallisuusriskien arviointiin, dokumentoidut turvallisuusohjeet sekä menettelytavat seurata ja kehittää turvallisuutta. AEO-viitekehystä eritellään tarkemmin luvuissa 3.2.1-3.2.16.

AEO-viitekehyksen valinta vertailuun on perusteltavissa monesta syystä. Koska AEO on toiminut koko tämän tutkimuksen alkulähteenä, tutkimuksessa on ollut mielekästä havainnoida AEO:n ja ISO 28000 -standardin sekä turvallisuuden hallinnan yleistyksen välisiä suhteita. Lisäksi AEO:n havaittiin viitekehysten kartoittamisvaiheessa viittaavan ISO 28000 -standardiin, johon perustuen se on soveltamisalaltaan ISO 28000 –standardia osin vastaava – AEO:n pääpaino on toimitusketjujen turvallisuudessa, mutta sen tavoitteena on olla kokonaisvaltainen turvallisuuden hallinnan viitekehys.

3.1.6 ISO 14001

ISO 14001:2004 ”Ympäristöjärjestelmät. Vaatimukset ja opastusta niiden soveltamisesta” –standardi määrittelee ympäristöjärjestelmää koskevat vaatimukset, joita soveltaen organisaatio voi laatia ja ottaa käyttöön toimintapolitiikan tavoitteineen, tarkoituksenaan vaikuttaa sellaisiin ympäristönäkökohtiin, joita se voi hallita. ISO 14001 on hallintajärjestelmästandardi, eikä se täten aseta itsessään erityisiä ympäristönsuojelun tason kriteerejä. (ISO 14001 2004, 10.)

Standardi on valittu osaksi vertailua sen ennaltaehkäisevän ja riskiperustaisen lähestymistavan takia. Toteuttaakseen tehokasta ympäristöjärjestelmää organisaation tulee tunnistaa mahdolliset ympäristöön vaikuttavat onnettomuus- ja hätätilanteet sekä luoda menettelytavat ennaltaehkäistä ja lieventää mahdollisia vaikutuksia. Organisaation on reagoitava mahdollisiin poikkeamiin ja luotava menettelytavat toimia poikkeustilanteissa. (ISO 14001 2004, 22.)

Standardia on haluttu käsitellä tutkimuksessa myös siksi, että kohdeorganisaation tiedettiin jo ennen tutkimuksen aloittamista soveltavan toimintaansa ISO 14001-standardinmukaisia menettelytapoja. Vertailun tulokset, standardien keskinäiset vastaavuudet, ovat täten hyödynnettävissä myös hallintajärjestelmien harmonisointia ja integraatiota varten. Standardia eritellään tarkemmin luvuissa 3.2.1-3.2.16.

3.2 Hallintajärjestelmän keskeiset elementit ja piirteet

Tunnistettaessa turvallisuuden hallintajärjestelmälle olennaisia elementtejä ja piirteitä, huomio tuli kiinnittää standardien ja muiden viitekehysten soveltamisalasta niiden taipumukseen ja vaatimuksiin ohjata organisaation johtamista menettelyineen. Vertailukelpoisten tutkimusjoukon saavuttamiseksi oli oleellista selvittää nimenomaan hallintajärjestelmän elementtejä, jotka ovat olennaisia soveltamisalasta riippumatta, paneutumatta yksittäisten viitekehysten soveltamisaloihin syvällisesti. Tästä syystä vertailussa on huomioitu myös soveltamisalaltaan muusta joukosta poikkeavat ISO 31000- ja ISO 9000-standardit. ISO 28000 -standardi esiintyy havainnollistamisen vuoksi myös liitteen 1 vertailutaulukoissa. Sitä ei kuitenkaan huomioida vertailuanalyysin johtopäätöksissä, sillä sitä ei voida tässä tutkimuksessa tarkastella vakiintuneena hallintajärjestelmästandardina. Standardia verrataan itsenäisesti muista viitekehyksistä yleistettyihin hallintajärjestelmien elementteihin luvussa 4.1.

SFS-ISO 31000:2011 *”Riskienhallinta. Periaatteet ja ohjeet”* ei soveltamisalansa puitteissa ole hallintajärjestelmästandardi, sillä se esittää yleisen toimintamallin riskienhallinnan perusteiden luomiseksi (ISO 31000 2011, 12). Riskienhallintaan kohdistuva viitekehys kuitenkin korostaa siihen lukeutuvin elementein riskienhallinnan ja turvallisuuden hallinnan välistä suhdetta sekä riskienhallinnan integroimista osaksi organisaation johtamisjärjestelmää. Kaikki tutkimuksessa käsitellyt viitekehykset asettavat Kansallista turvallisuudenauditointikriteeristöä ja ISO 9001 -standardia lukuun ottamatta vaatimuksia turvallisuuden hallinnan menettelyille riskienarviointiin perustuen. Viitekehykset eivät aseta tarkoin määriteltyjä toimenpiteitä vaan menettelyt ovat riittäviä, mikäli ne laskevat havaitut riskit riskienarviointiin perustuen hyväksyttävälle tasolle

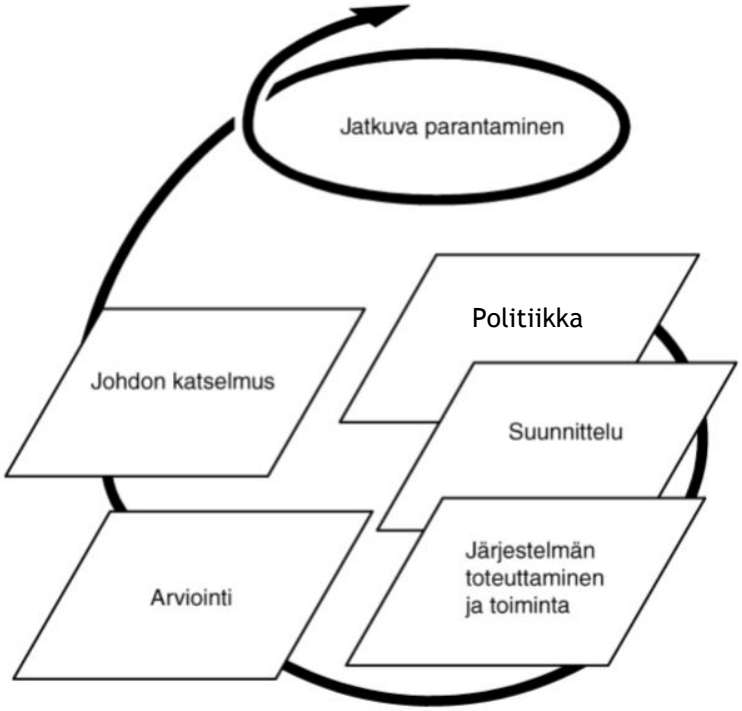
ISO 9001-standardi asettaa määritelmiä ja vaatimuksia laadunhallintajärjestelmille. Standardin tarkoituksena on luoda organisaatiolle lisäarvoa parantamalla asiakastyytyväisyyttä. Laadunhallintajärjestelmien suunnittelulla, toteuttamisella ja ylläpidolla yritys lisää mahdollisuuttaan toimittaa tuotetta tai palvelua, joka täyttää sidosryhmien asettamat vaatimukset kaikissa tilanteissa. (ISO 9001 2008, 10.) ISO 9001 eroaa muista tarkastelluista viitekehyksistä myös prosessi- ja asiakastyytyväisyyteen keskittyvään lähestymistapansa vuoksi, jossa toimintajärjestelmä perustuu prosessien tunnistamiseen, hallintaan ja suorituskyvyn mittaamiseen. Muut käsitellyt viitekehykset perustuvat riskiperusteiseen lähestymistapaan, jonka keskiössä

ovat toimintoon kohdistuvien riskien ja uhkien tunnistaminen, jotka määrittelevät tarpeet toimintajärjestelmän toteuttamiselle. ISO 9000-standardin on valittu vertailuun sen hallintajärjestelmäpiirteiden ja muihin viitekehyksiin läheisten suhteiden vuoksi.

Hallintajärjestelmille oleellista on jatkuvan parantamisen prosessimainen PDCA-toimintamalli, ”Plan-Do-Check-Act/Suunnittele-Toteuta-Arvio-Toimi”. ISO 9001-standardin mukaan (laadun)hallintajärjestelmän toteuttaminen sisältää seuraavia vaiheita:

1. Sidosryhmien tarpeiden ja odotusten määrittäminen (vrt. uhkien ja riskien tunnistaminen)
2. (Laatu)politiikan ja –tavoitteiden asettaminen
3. Prosessien, resurssien ja vastuiden määrittäminen tavoitteiden saavuttamiseksi
4. Menettelyjen luominen vaikuttavuuden ja tehokkuuden mittaamiseksi
5. Menetelmien luominen poikkeamien ennaltaehkäisemiseen ja poikkeamatilanteisiin
6. (Laadun)hallintajärjestelmän jatkuvan parantamisen menettelyn luominen ja soveltaminen (ISO 9008 2008, 12).

Jatkuvan parantamisen prosessia voidaan kuvata oheisin mallin mukaisesti (ks. Kuvio 3).



Kuvio 3 Hallintajärjestelmä prosessina (ISO 14001 2004, 8; OHSAS 18001 2007, 12; ISO 28000 2007, 14 muokattu).

Tutkija esittää hallintajärjestelmän keskeisiksi elementeiksi alaluvuissa 3.2.1-3.2.16 eriteltyjä teemoja, joita verrataan kootusti ISO 28000 -standardiin luvussa 4.1, taulukossa 1. Teemat eli elementit on koostettu vertailemalla tutkimuksen aineistoina käytettyjä viitekehyksiä.

Elementtien muodostamisen kriteeriksi on asetettu, että elementin perustana olevien vaatimusten pitää löytyä yli puolista, yhteensä kahdeksasta tarkastellusta viitekehyksestä. Seuraavissa luvuissa kuvataan elementtien keskeistä sisältöä ja tarkoitusta sekä viitekehysten vastaavuuksia yksittäisten osa-alueiden suhteen.

3.2.1 Politiikka

Turvallisuuspolitiikka on johdon julkilausuma turvallisuuden merkityksestä organisaatiolle, joka ohjaa organisaation turvallisuuteen varattuja resursseja sovittujen periaatteiden mukaisesti. Se määrittelee, sisältäen muttei rajoittuen, suuret linjaukset turvallisuustyön painopisteistä ja tavoitteista sekä vastuista, velvoitteista ja valtuuksista. Turvallisuuspolitiikalla halutaan viestiä, että turvallisuustoiminta on osa liiketoimintaa, jota halutaan jatkuvasti kehittää muun muassa laatujohtamisen keinoin. (Kerko 2001, 44; Leppänen 2006, 177.)

Vertailun tuloksena (ks. liite 1, taulukko 1) voidaan todeta, että kaikki viitekehykset velvoittavat toimintaa ohjaavan politiikan laatimista. Politiikan tulee olla organisaation luonteelle ja toiminnan laajuudelle tarkoituksenmukainen, ajantasainen sekä johdon hyväksymä. Tarkastelun tuloksena voidaan siis todeta toimintapolitiikan olevan olennainen osa hallintajärjestelmiä.

3.2.2 Riskien- ja toimintaympäristön arviointi

Riskienhallinnalla ymmärretään yritysmaailmassa yleisesti menettelyjä, joilla pyritään suojaamaan yrityksen tulosta ei-toivotuilta tapahtumilta. Toisaalta, se kattaa myös liiketoiminnan mahdollisuuksien tunnistamisen, arvioinnin ja hallinnan. Yritystoiminnan suojaamiseen liittyvässä riskienhallinnassa korostetaan toiminnan jatkuvuutta ja häiriöttömyyttä, tehokkuutta, laatua sekä turvallisuutta. (Ilmonen ym. 2010, 17.)

Organisaatiosta ja toimintaympäristöstä riippuen, turvallisuuden hallinta voi olla osana riskienhallintaa tai päinvastoin. Turvallisuuden hallinta on ennen kaikkea riskienarviointiin perustuva prosessi, joka ei palvele tarkoitustaan ja päämääriään, mikäli taustalla ei ole toimivaa riskienhallinnan mekanismia. Toisaalta, osana turvallisuusriskienhallintaa suoritettavat korjaavat toimenpiteet ja suojausmenettelyt, sekä niiden valvonta ja kehittäminen, ovat turvallisuuden hallintaa puhtaimmillaan. Sekä riskienhallinnalla että turvallisuuden hallinnalla pyritään vaikuttamaan samoihin tavoitteisiin. (Kerko 2001, 57-58; Leppänen 2006, 14.) Leppänen (2006, 14) esittääkin, että turvallisuuden ja riskienhallinnan välisen hierarkian pohtimiseen on yhteisen päämäärän eli häiriöttömän toiminnan kannalta epäolennaista käyttää liialti resursseja; tavoitteet pyritään saavuttamaan riippumatta häiriötekijöiden laadusta tai suoritettavista suojausmenettelyistä.

ISO 31000 –standardin (2011) mukaan riskienhallinnan toteuttaminen antaa mahdollisuuden muun muassa:

- lisätä tavoitteiden saavuttamisen todennäköisyyttä
- tukea proaktiivista johtamista
- noudattaa viranomaisen ja lainsäädännön asettamia vaatimuksia
- kehittää raportointia
- kehittää organisaation hallintotapaa
- parantaa operatiivista tehokkuutta
- parantaa terveyteen ja turvallisuuteen liittyvän toiminnan sekä ympäristön suojelun tasoa
- kehittää vahingontorjuntaa ja häiriötilanteiden hallintaa
- vähentää tappioiden määrää. (ISO 3100 2011, 7-8.)

Yllä lueteltuja riskienhallinnan tuottamia hyötyjä voidaan pitää ominaisina myös turvallisuuden hallinnan toteuttamisen yhteydessä. Riskienhallinta on turvallisuuden hallintajärjestelmän toteuttamisen ytimessä. Riskiperusteiset toimintajärjestelmät perustuvat toimintaympäristön analysointiin ja organisaatioon ja sen toimintoihin kohdistuvien riskien ja uhkien tunnistamiseen, jotka luovat pohjan hallintajärjestelmän menettelyille ja ominaisuuksille.

Vertailun perusteella (ks. liite 1, taulukko 2) voidaan todeta, että ISO 9001-standardia lukuun ottamatta kaikki viitekehykset sisältävät tai kokonaisuudessaan rakentuvat uhkien, riskien ja/tai vaarojen tunnistamiselle. Tunnistetut uhat ovat hallintajärjestelmän keskiössä, joihin järjestelmällä menettelyineen pyritään vaikuttamaan. Poikkeuksena muista viitekehyksistä esiintyy myös ISO 27001, joka ei perustu uhkien ja riskien tunnistamiselle. Kyseinen standardi noudattelee ISO 9001-standardin mukaista prosessimaista mallia, jonka keskiössä on lainsäädännöllisten ja ulkoisten osapuolien asettamien vaatimusten tunnistaminen ja niihin vastaaminen. Hallintajärjestelmän menettelyt tulee kuitenkin rakentaa turvallisuusriskien arviointiin perustuen. (ISO 27001 2006, 8; 10-18.) Tarkastelun tuloksena riskienarvioinnin voidaan todeta olevan oleellinen osa turvallisuuden hallintajärjestelmää.

3.2.3 Lakisääteiset ja ulkoiset vaatimukset

Organisaation on tunnistettava liiketoimintaan ja turvallisuuden hallintajärjestelmään sekä sen sisältämiin menettelyihin kohdistuvat lakisääteiset-, viranomais- ja muut ulkoiset vaatimukset (kuten asiakasvaateet ja vakuutusyhtiöiden vaatimat kontrollit), Organisaation on suunniteltava ja toteutettava menettelytapoja vaatimusten täyttämiseksi. (ISO 28000 2007, 18.) Lakisääteiset ja ulkoiset vaatimukset ovat sidonnaisia viitekehyksen soveltamisalaan.

Vertailun perusteella (ks. liite 1, taulukko 3) voidaan todeta, että kaikki tarkastellut viitekehykset ottavat kantaa lakisääteisten ja ulkoisten vaatimusten tunnistamiseen, soveltamiseen ja noudattamiseen. Joukosta ISO 9001 –standardi on ainoa, joka ei käsittele lainsäädäntöä johtamisen tai liiketoiminnan näkökulmasta, vaan se määrittelee ainoastaan tuotteeseen liittyvien ulkoisten vaatimusten osalta. Soveltamisalastaan riippuen viitekehyksissä on oma lähestymistapansa tai sävynsä lainsäädännön ja ulkoisten vaatimusten käsittelyyn. Esimerkiksi ISO 27001 painottaa lakisääteisten ja ulkoisten tietoturvavaatimusten keskeisyyttä tietoturvallisuuden hallintajärjestelmän perustana. AEO:n ehdottomina vaatimuksina on, että organisaatio on taloudellisesti vakavarainen ja se noudattaa tullauskäytännöissään asetettuja vaatimuksia, missä taas ISO 14001 –standardin määritelmät rajoittuvat ympäristönäkökohtiin vaikuttaviin lainsäädännöllisiin ja ulkoisiin vaatimuksiin. Myös ISO 31000 huomioi sivuten lakisääteisten ja ulkoisten vaatimusten asettamat vaatimukset. Standardin (2009, 28) mukaan organisaation on arvioitava ja ymmärrettävä sisäinen ja ulkoinen toimintaympäristönsä (sisältäen lainsäädännön ja sidosryhmien vaatimukset), jotta riskienhallinnan puitteisiin vaikuttavat tekijät huomioidaan hallintajärjestelmässä. Tarkastelun tuloksena voidaan todeta, että lainsäädännön ja ulkoisten vaatimusten tunnistaminen, soveltaminen ja noudattaminen ovat oleellinen osa turvallisuuden hallintajärjestelmää.

3.2.4 Tavoiteasetanta

Tavoiteasetannan tarkoituksena on johtaa politiikoista selkeästi määriteltyjä ja mitattavissa olevia päämääriä ja tavoitteita, jotka ohjaavat organisaation toimintaa. Päämäärät ja tavoitteet tulee arvioida ja päivittää määräajoin sekä tiedottaa asianosaiselle henkilökunnalle ja kolmansille osapuolille. Tavoitteiden määrittelemisessä tulee huomioida muun muassa:

- lakisääteiset ja muut ulkoiset vaatimukset
- turvallisuusuhat ja –riskit
- taloudelliset, toiminalliset ja liiketoiminnalliset vaatimukset
- teknologiset ja muut vaihtoehdot. (ISO 28000 2007, 18; Leppänen 2006, 176-177.)

Vertailun perusteella (ks. liite 1, taulukko 4) voidaan todeta, että kaikki tarkastellut viitekehykset vaativat organisaatiolta tavoitteiden ja päämäärien asettamista. Viitekehykset lähestyvät tavoiteasetantaa KATAKRI:a, AEO:ta ja ISO 28000 -standardia lukuun ottamatta omasta soveltamisalastaan riippuen. Edellä luetellut viitekehykset sen sijaan linjaavat tavoiteasetannan koskemaan yleisemmällä tasolla laveammin ”turvallisuuden hallintaa”. Tarkastelun tuloksena voidaan todeta, että tavoitteiden ja päämäärien asettaminen on yksi turvallisuuden hallinnan oleellisista elementeistä.

3.2.5 Organisaation vastuut ja valtuudet

Hallintajärjestelmän tavoitteiden ja päämäärien saavuttamiseksi organisaation on määriteltävä, tiedotettava ja dokumentoitava menettelyihin liittyvät roolit vastuineen ja valtuuksineen. Vastuiden ja valtuuksien määrittämisen yhteydessä korostetaan yleisesti myös organisaation johdon toimenkuvan ja vastuiden määrittely, johdon sitoutumisen varmistamiseksi ja riittävien toimeenpanovaltuuksien ja resurssien takaamiseksi.
Vertailun perusteella (ks. liite 1, taulukko 5) voidaan todeta, että kaikki tarkastellut viitekehykset ottavat kantaa organisaation vastuiden ja valtuuksien määrittämiseen. Kaikki viitekehykset linjaavat, että vastuiden tulee kattaa koko organisaation ja, että hallintajärjestelmän edellyttämien toimenpiteiden koordinoimiseksi ja toteuttamiseksi sekä riittävien resurssien takaamiseksi vastuuhenkilöillä tulee olla riittävät toimeenpanovaltuudet. ISO- ja OHSAS-standardit täsmentävät lisäksi, että vastuiden on ulotuttava ylimpään johtoon asti. Tarkastelun tuloksena voidaan todeta, että organisaation vastuiden ja valtuuksien määrittäminen on oleellinen osa hallintajärjestelmien rakentamista ja ylläpitoa

3.2.6 Johdon sitoutuminen

Johdon sitoutuminen (ISO 9000 mukaan ”johtajuus”) on osa hallintajärjestelmän toteuttamista. Johtajien tulee määrittää organisaation tarkoitus ja suunta sekä luoda ja ylläpitää organisaatiossa ilmapiiriä, joka mahdollistaa henkilöstön täysipainoisen osallistumisen tavoitteiden saavuttamiseen (ISO 9000 2005, 9). Johdon tehtävän on myös suorittaa järjestelmällisiä katselmuksia hallintajärjestelmän soveltuvuuden, riittävyyden, vaikuttavuuden ja tehokkuuden arvioimiseksi (IS0 9000 2005, 18). Kerkon (2001) mukaan aito sitoutuminen edellyttää muun muassa johdon osallistavaa työtapaa ja turvallisuusasioista viestimistä sekä selkeää ja läpinäkyvää organisaatiota, jossa jokaisen vastuut ja tehtävät on selkeästi määritelty.

Vertailun perusteella (ks. liite 1, taulukko 6) voidaan todeta, että AEO:ta lukuun ottamatta kaikki viitekehykset edellyttävät joko välitöntä tai välillistä johdon sitoutumista hallintajärjestelmiin. Välittömällä sitoutumisella viitataan tässä tapauksessa osassa viitekehyksiä esiintyvään ”johdon sitoutuminen” –vaatimukseen ja josta viitekehykset erikseen määrittelevät. Välillisellä sitoutumisella sen sijaan tarkoitetaan viitekehyksissä esiintyviä yhtä tai joukkoa yksittäisiä vaatimuksia, jotka edellettävät organisaation johdolta a) vastuun kantamista ja/tai b) toimenpiteiden suorittamista hallintajärjestelmän osalta. Johdon sitoutuminen ilmenee viitekehyksissä muun muassa vastuiden ja roolien kautta sekä hallintajärjestelmien liittämisenä osaksi johdon katselmointeja.

Ainoastaan AEO ei suoraan linjaa johdon sitoutumisesta. AEO-suuntaviivoissa kuitenkin suositellaan, että etenkin suurissa organisaatioissa yhteyshenkilöksi eli AEO:sta vastaavaksi henki-

löksi nimetään johtotason henkilö, jolla on valtuudet koordinoida ja toteuttaa asianmukaisia turvatoimia ja joka kantaa kokonaisvastuun kaikista turvallisuustoimista yrityksen asiaankuuluvissa yksiköissä (Euroopan komissio 2012, 10; 15). Edellytys johdon sitoutumiselle ilmenee myös aiempana tarkastellun politiikan kautta, sillä AEO velvoittaa, että organisaatiossa tulee olla turvallisuuspolitiikka. Tarkastelun tuloksena voidaan todeta, että johdon sitoutuminen on oleellinen osa hallintajärjestelmiä.

3.2.7 Resursointi

Resursoinnilla tarkoitetaan rahallisen, työpanoksen tai muun oleellisen panoksen varaamista asetettujen tavoitteiden saavuttamiseksi. Hallintajärjestelmissä resursoinnilla tarkoitetaan yleisesti henkilö- ja rahallisten resurssien varaamista, jotka kytkeytyvät henkilöiden asemaan organisaatiossa ja tätä kautta riittäviin toimeenpanovaltuuksiin.

Vertailun perusteella (ks. liite 1, taulukko 7) voidaan todeta, että kaikki viitekehykset ottavat kantaa resursoimiseen. Kaikki viitekehykset määrittelevät yhtenäisesti, että hallintajärjestelmän toteuttamiseksi ja siinä asetettujen tavoitteiden saavuttamiseksi tulisi varmistaa muun muassa valtuuksien määrittämisen kautta riittävät resurssit. Tarkastelun perusteella voidaan todeta, että resursointiin liittyvien menettelyjen määritteleminen on olennainen osa hallintajärjestelmiä.

3.2.8 Toiminnan ohjaus

Leppäsen (2006, 25,175) mukaan turvallisuustoiminnan ja riskienhallinnan tulee linkittyä kiinteänä osana organisaation tavoitteisiin ja strategiaan. Sekä turvallisuuden hallinnalla, riskienhallinnalla että laatujohtamisella on samat tavoitteet; toiminnan häiriöttömyyden varmistaminen ja täten tuotteiden ja/tai palveluiden laadun takaaminen. Toiminnan ohjauksella tarkoitetaan niiden toimintojen määrittelyä ja hallintaa, joilla edellä mainitut tavoitteet saavutetaan.

Vertailun perusteella (ks. liite 1, taulukko 8) voidaan todeta, että kaikki tarkastellut viitekehykset ottavat kantaa toiminnan ohjaukseen, soveltamisalansa puitteissa. ISO-standardien linjaukset ovat lähes identtisiä, pois lukien soveltamisaloista johtuvat eroavuudet. ISO 28000 poikkeaa muista ISO-standardeista siinä, että se määrittelee toiminnan ohjauksen lisäksi ”turvallisuuden hallinnan ohjelmista”, joiden tarkoituksena on hallita ja seurata toiminnan ohjaukseen liittyviä prosesseja.

KATAKRI:ssa toiminnan ohjaukseen viittaa ”Turvallisuuden vuotuinen toimintaohjelma”, joka korotetun tason (III) mukaan on organisaation toimintaohjelma, joka kattaa turvallisuusjoh-

tamisen, henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Toimintaohjelma voi olla erillinen dokumentti tai se voi olla sisällytettynä organisaation toimintasuunnitelmaan. (Puolustusministeriö 2011, 14.) AEO puolestaan linjaa toiminnan ohjauksesta hyvin laveasti: *"Toimijan, joka hakee AEO-asemaa ja pyrkii saamaan sen, on otettava huomioon, että sen on "hallittava" liiketoimintaansa"* (Euroopan komissio 2012, 10).

Kaikki viitekehykset linjaavat kuitenkin toiminnan ohjauksesta periaatetasolla samalla tavalla: Organisaation on luotava konkreettisia hallintotoimenpiteitä, joilla politiikan määrittelyt, turvallisuus- ja/tai laatutavoitteet täytetään ja joilla voidaan puuttua tunnistettuihin uhkiin ja riskeihin ja/tai laatupoikkeamiin johtaviin tapahtumiin. Tarkastelun tuloksena voidaan todeta, että toiminnan ohjaus tavoitteiden ja päämäärien saavuttamiseksi on oleellinen osa hallintajärjestelmiä.

3.2.9 Pätevyys, koulutus ja tietoisuus

Hallintajärjestelmän toteuttamisen kannalta on oleellista, että asianosaisilla henkilöillä on tehtäviinsä, vastuihinsa ja valtuuksiinsa nähden riittävä tietoisuus järjestelmän edellyttämistä menettelyistä. Mahdollisten koulutusten tai muiden tietoisuutta lisäävien menettelyiden suunnittelemiseksi sekä organisaatioiden koulutustarpeiden tunnistamiseksi, tulisi määritellä millaisia pätevyyksiä kuhunkin rooliin vaaditaan. Koulutusten suunnitellussa olisi myös huomioitava organisaation tavoitteet, vastuut, kyvyt, kielitaito- ja koulutustasot sekä riskit, jotka johtuvat menettelyistä poikkeamisesta. (ISO 9001 2008, 22; OHSAS 18001 2007, 26.)

Vertailun perusteella (ks. liite 1, taulukko 9) voidaan todeta, että kaikki tarkastellut viitekehykset ottavat kantaa pätevyyden, koulutuksen ja tietoisuuden roolista osana hallintajärjestelmiä. Ainoastaan riskienhallinnan standardi ISO 31000 ei suoraan määrittele organisaation kouluttamisesta, mutta se kuitenkin mainitsee sivuten tarvittavan koulutuksen järjestämisestä osana riskienhallinnan puitteiden toteuttamista. Tarkastelun tuloksena voidaan todeta, että asianosaisten henkilöiden tarpeenmukainen kouluttaminen ja tietoisuuden lisääminen on olennainen osa hallintajärjestelmän toteuttamista.

3.2.10 Viestintä

ISO 28000 -standardin (2007, 22) mukaan organisaation tulee varmistaa, että olennaiset turvallisuuden hallinnan tiedot on tiedotettu asianmukaisten henkilöiden toimesta asianmukaisen henkilöstön lisäksi myös tarvittaville alihankkijoille ja muille sidosryhmille. Viestinnän tarkoituksena on lisätä tietoisuutta hallintajärjestelmän edellyttämistä menettelyistä, mutta myös viestittää organisaatiokulttuurista.

Vertailun perusteella (ks. liite, taulukko 10) voidaan todeta, että kaikki viitekehykset ottavat kantaa hallintajärjestelmiin liittyvään viestintään, ISO 27001-standardia lukuun ottamatta. Standardissa (2005, 25) todetaan ainoastaan, että henkilöstön on oltava tietoinen tietoturvallisuuteen liittyvistä tehtävistään ja vastuistaan. Menettely painottuu kuitenkin enemmän koulutuksellisiin tekijöihin, viestinnän sijasta.

Kaikki viestintää käsittelevät viitekehykset jakavat viestinnän sisäiseen ja ulkoiseen viestintään. Tarkastelun tuloksena voidaan todeta, että hallintajärjestelmien menettelyistä viestiminen sekä organisaation sisäisesti että ulkoisesti, on olennainen osa hallintajärjestelmien toteuttamista.

3.2.11 Dokumentointi

Hallintajärjestelmät tulee menettelyineen dokumentoida, jotta niitä voidaan toistuvasti tarkastella ja käsitellä samoin tuloksin. Dokumentointi luo pohjan järjestelmän systemaattiselle hallinnalle sekä sisäiselle että ulkoiselle kommunikoinnille.

Vertailun perusteella (ks. liite 1, taulukko 11) voidaan todeta, että kaikki viitekehykset ottavat kantaa hallintajärjestelmän dokumentointiin. ISO-standardit linjaavat ISO 9001-standardiin (2008, 16) perustuen, että hallintajärjestelmän tulee perustua järjestelmälliseen dokumentaatioon ja ohjeistukseen. Hallintajärjestelmissä käytettäviä asiakirjoja ovat (sisältäen, muttei rajoittuen):

- hallintajärjestelmän rakennetta ja sisältöä kuvaavat asiakirjat
- suunnitelmat, jotka kuvaavat miten hallintajärjestelmää sovelletaan tiettyihin toimintoihin
- spesifikaatiot, jotka määrittävät vaatimuksia tuotteille tai palveluille
- oppaat, jotka sisältävät suosituksia ja ehdotuksia
- menettelyohjeet, työohjeet ja kuvaukset, jotka antavat informaatiota toimintojen ja prosessien johdonmukaiseen toteuttamiseen
- tallenteet, jotka antavat objektiivista näyttöä suoritetuista toimenpiteistä tai saavutetuista tuloksista.

Viitekehyksistä AEO linjaa dokumentaation laadusta laveasti: ”Kaikki menettelyt on dokumentoitava ja asetettava tulliviranomaisten saataville AEO-vaatimusten tarkastuksessa, ja ne tarkastetaan aina yrityskäynnillä”. (Euroopan komissio 2012, 14.) Tarkastelun tuloksena voidaan todeta, että hallintajärjestelmän rakenteen, sisällön ja kattavuuden kuvaaminen ja dokumentoiminen menettelyineen on oleellinen osa hallintajärjestelmiä.

3.2.12 Asiakirjojen ja tallenteiden hallinta

Asiakirjojen ja tallenteiden hallinnalla tarkoitetaan menettelyä tunnistaa, kerätä, arvioida, seurata ja dokumentoida sellaisia tallenteita, jotka mahdollistavat organisaatiossa tehokkaan suunnittelun, toteutuksen ja prosessien hallinnan (ISO 28000 2007, 22.) Tallenteiden hallintaa liittyy olennaisesti myös organisaation raportointimenettelyt, jotka ovat osa tallenteiden keräämistä ja seurantaa. Turvallisuuden hallinnan kannalta oleellisia tallenteita ovat sisältäen, muttei rajoittuen muun muassa seuraavat:

- turvallisuustapahtumat ja -poikkeamat
- reklamaatioita koskevat tallenteet
- koulutustallenteet
- prosessin tarkkailua koskevat tallenteet
- tarkastus-, kunnossapito- ja kalibrointitallenteet
- olennaiset urakoitsija- ja toimittajatallenteet
- vahinkoraportit
- hätätilannevalmiuden testaamista koskevat tallenteet
- auditointitulokset
- johdon katselmusten tulokset
- ulkoista viestintää koskevat päätökset
- tallenteet soveltuvista lakisääteisistä vaatimuksista ja vaatimusten mukaisuudesta
- viestintä sidosryhmien kanssa. (ISO 14001 2004, 40; ISO 28001 2007, 16.)

Vertailun perusteella (ks. liite 1, taulukko 12) voidaan todeta, että tarkastellut viitekehykset ottavat kantaa tallenteiden hallintaan AEO:ta lukuun ottamatta. ISO-standardit määrittelevät tallenteiden hallinnasta lähes identtisesti aiempana esitetyn listauksen mukaisesti, soveltamisaloista johtuvat erot pois lukien. KATAKRI määrittelee kysymysten A 701 ja A 702 korotetulla tasolla (III), että organisaatiolla tulee olla järjestelmä, joka sisältää turvallisuusrekisterit, omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat ja jolla organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain. (Puolustusministeriö 2011, 37.)

AEO on joukon ainoa, joka ei suoraan määrittele tallenteiden hallinnasta. Kyseinen viitekehys kuitenkin edellyttää menettelyjä turvallisuustoiminnan seuraamiseksi, jonka suorittamiseksi tallenteet ovat avainasemassa. Tarkastelun tuloksena voidaan todeta, että tallenteiden hallinta on organisaation aktiivisen ja jatkuvan toiminnan kannalta oleellista sekä hallintajärjestelmille keskeinen elementti.

3.2.13 Toiminta poikkeustilanteissa

Toiminnan häiriöttömän jatkumisen varmentamiseksi sekä mahdollisten poikkeamatilanteiden aiheuttamien seurausten lieventämiseksi, organisaation tulisi luoda, toteuttaa ja ylläpitää menettelyjä mahdollisten poikkeus- ja hätätilanteiden tunnistamiseen ja niissä toimimiseen. Näiden menettelyiden suunnittelussa tulee huomioida asianmukaiset sidosryhmät sekä tarvittavat testaus- ja päivittämismenettelyt. (ISO 28000 2007, 24; OHSAS 18001 2007, 30.) Vertailun perusteella (ks. liite 1, taulukko 13) voidaan todeta, että kahdeksasta tarkastellusta viitekehyksestä kaksi (ISO 27001 ja ISO 31000) ei aseta poikkeustilanteiden hallinnalle vaatimuksia lainkaan ja yksi vain osittain ja välillisesti (AEO). AEO määrittelee, että organisaation tulee laatia turvallisuussuunnitelma, mutta sen pakollisia sisältövaatimuksia ei kuitenkaan ole eritelty. AEO kuitenkin määrittelee tietoturvallisuuden jatkuvuudenhallinnan suhteen, että organisaatiolla tulee olla menettelytavat tietojärjestelmien toimintahäiriöiden varalle ja häiriöistä palautumiseen.

Muut tarkastellut viitekehykset ovat kuitenkin yksimielisiä poikkeamatilannemenettelyiden suhteen. Joukosta ISO 9001 kuitenkin linjaa soveltamisalansa johdosto poikkeamatilanteiden hallinnan koskemaan poikkeavan tuotteen ohjausta, jolla kyseinen standardi viittaa vaara- ja hätätilanteiden sijasta menettelyihin, joilla ei-vaatimustenmukainen tuote tunnistetaan ja ohjataan siten, ettei se tahattomasti jakeluun eikä sitä oteta käyttöön. (ISO 9001 2008, 36.) Tarkastelun tuloksena voidaan todeta, että etenkin turvallisuutta käsittelevissä hallintajärjestelmissä poikkeustilanteiden hallinta on olennainen osa hallintajärjestelmin toteuttamista.

3.2.14 Poikkeamat, korjaavat ja ennaltaehkäisevät toimenpiteet

OHSAS-standardin (2007, 32) mukaan organisaation on luotava, toteutettava ja ylläpidettävä menettelyjä, joilla voidaan käsitellä mahdollisia poikkeamia sekä huolehditaan korjaavista ja ennaltaehkäisevistä toimenpiteistä. Vaatimukset viittaavat, että organisaation olisi panostettava proaktiiviseen toimintaan ja että poikkeamien tutkiminen sekä korjaavat ja ennaltaehkäisevät toimenpiteet ovat hallintajärjestelmien jatkuvan parantamisen kannalta oleellinen elementti.

Vertailun perusteella (ks. liite 1, taulukko 14) voidaan todeta, että ISO 31000-standardia lukuun ottamatta kaikki viitekehykset ottavat kantaa poikkeamien sekä korjaavien ja ennaltaehkäisevien menettelyiden asettamiseen. Turvallisuutta käsittelevät viitekehykset painottavat myös, että ennen ennaltaehkäisevien ja korjaavien toimenpiteiden suorittamista tulee arvioida uhat ja riskit, joita suunnitellut toimenpiteet mahdollisesti aiheuttavat. Toteutettuja korjaavia ja ennaltaehkäiseviä toimenpiteitä puolestaan tulee seurata ja katselmoida tehokkuuden arvioimiseksi. Tarkastelun tuloksena voidaan todeta, että menettelyjen luominen

poikkeamien tunnistamiseksi, korjaamiseksi ja ennaltaehkäisemiseksi on oleellinen osa hallintajärjestelmien toteuttamista.

3.2.15 Suorituskyvyn mittaaminen

Hallintajärjestelmän suorituskyvyn mittaamisella tarkoitetaan hallintajärjestelmään sisältyvien menettelyiden tehokkuuden ja vaikuttavuuden tarkastelua. Suorituskyvyn mittaaminen eroaa hallintajärjestelmän puitteiden arvioinnista oleellisesti siinä, että se ei mittaa hallintajärjestelmän toimivuutta vaan hallintajärjestelmässä määriteltyjen menettelyiden vaikutusta organisaation prosesseihin ja toimintaan. Mittariston suunnittelussa, luomisessa ja toteuttamisessa tulisi huomioida, että käytössä olisi sekä laadullisia että määrällisiä mittareita, ennakoivia ja reagoivia mittareita ja tärkeimpänä, mittareita, jotka soveltuvat politiikkojen, päämäärien ja tavoitteiden asettamien parametrien seurantaan (ISO 28000 2007, 26).

Vertailun perusteella (ks. liite 1, taulukko 15) voidaan todeta, että ISO 27001-standardia lukuun ottamatta kaikki viitekehykset ottavat kantaa hallintajärjestelmän suorituskyvyn mittaamiseen. Vaikka ISO 27001 ei aseta turvallisuuden suorituskykymittareille vaatimuksia, vaatii se kuitenkin turvamekanismien tehokkuuden mittaamista, jotta varmistutaan, että turvallisuusvaatimukset on täytetty (ISO 27001 2006, 18). Mittaamisessa ei standardin mukaan siis keskitytä mittaamaan vaikuttavuutta vaan vaatimusten täyttämistä. Tarkastelun tuloksena voidaan todeta, että prosessien ja suorituskyvyn mittaaminen on olennainen osa hallintajärjestelmien toteuttamista.

3.2.16 Hallintajärjestelmän arviointi

Järjestelmän arviointi ja jatkuva parantaminen ovat olennainen osa toteuttamista. Arvioinneilla pyritään toteamaan onko tarvittavat prosessit tunnistettu, määritelty ja vastuutettu asianmukaisesti, onko menetelty sovitulla tavalla ja pidetäänkö menettelyjä yllä sekä ovatko prosessit vaikuttavia vaadittujen tulosten saavuttamiseksi. Arvioinnit voivat sisältä erilaajuisia toimintoja kuten auditointeja, katselmuksia ja itsearviointeja (ISO 9000 2005, 16). Arviointeihin perustuen laadunhallintajärjestelmää tulee kehittää jatkuvasti asettamalla, suorittamalla, mittaamalla ja uudelleen arvioimalla sekä vakiinnuttamalla parantamistoimenpiteitä (ISO 9000 2005, 18).

Vertailun perusteella (ks. liite 1, taulukko 16) voidaan todeta, että kaikki tarkastellut viitekehykset ottavat kantaa hallintajärjestelmän arviointiin. Myös hallintajärjestelmien arviointiin liittyvät keskeiset menettelyt ovat viitekehyksestä riippumatta samoja. Menettelyiden tarkoituksena on tiivistetysti varmistaa, että hallintajärjestelmä vastaa tarkoitustaan ja siinä asetetut menettelyt ovat oikein kohdistettuja ja tehokkaita. Tarkastelun tuloksena voidaan todeta,

että hallintajärjestelmän arviointi on olennainen osa hallintajärjestelmiä ja niiden toteuttamista.

4 ISO 28000 hallintajärjestelmästandardina

ISO 28000 -standardin soveltuvuutta kokonaisvaltaiseksi turvallisuuden hallintajärjestelmäksi on arvioitu tutkimuksessa kolmella metodilla. Standardia verrataan viitekehysten vertailuanalyysin tuloksiin, jotka määrittävät hallintajärjestelmälle keskeiset elementit. Standardia on arvioitu myös sisällönanalyysin keinoin, jonka tarkoituksena on pyritty selvittämään standardissa asetetut rajoitteet sen soveltamisalaan ja laajuuteen liittyen. Kolmantena metodina on käytetty asiantuntijahaastattelua, jolla on pyritty tuomaan tutkimukseen tutkijasta ja tutkijan suorittamista johtopäätöksistä riippumaton näkökanta. Tutkimusmenetelmien tuloksia kuvataan jäljempänä seuraavissa alaluvuissa. ISO 28000 -standardin soveltuvuutta arvioidaan tutkimustulosten yhteenvetona luvussa 4.4.

4.1 Standardin suhde hallintajärjestelmiin

Kaikki tutkimuksessa tarkastellut viitekehykset sisältävät muutamaa yksittäistä poikkeusta lukuun ottamatta samat elementit. Kuten jo aiempana esitetystä vertailuanalyysistä voidaan todeta, myös ISO 28000 täyttää useimpien tarkasteltujen viitekehysten tavoin kaikki hallintajärjestelmälle oleelliset piirteet. Yhteenvetona lukujen 3.2.1-3.2.16 vertailuanalyysistä tehtyjen yleistysten ja johtopäätösten perusteella tutkija esittää tarkasteltujen viitekehysten valossa hallintajärjestelmille keskeisiksi elementeiksi taulukossa 1 esiintyviä ”Hallintajärjestelmän elementtejä”. Vertailuanalyysin perusteella voidaan todeta, että järjestelmätasolla ISO 28000 -standardi täyttää kaikki kokonaisvaltaiselle johtamis- ja/tai hallintajärjestelmälle asetetut vaatimukset.

Hallintajärjestelmän elementti	ISO 28000 (Kyllä/Ei – Viite)
Ylimmän johdon vahvistama hallintapolitiikka	Kyllä. (ISO 28000 2007, 14).
Menettelytavat jatkuvalle hallintaan liittyvien uhkien ja riskien tunnistamiselle ja arvioimiselle sekä johdon valvontatoimenpiteiden tunnistamiselle ja toteuttamiselle	Kyllä. (ISO 28000 2007, 16).
Hallintaan kohdistuvien lakisääteisten ja ulkoisten vaatimusten tunnistaminen	Kyllä. (ISO 28000 2007, 18).
Tavoiteasetanta	Kyllä. (ISO 28000 2007, 18).
Hallintaohjelmat ja toiminnanohjaus, joilla saavutetaan hallintapolitiikan päämäärät ja tavoitteet ja joita ylläpidetään ja arvioidaan määräajoin	Kyllä. (ISO 28000, 20, 24).
Organisaation vastuiden ja valtuuksien määrittäminen	Kyllä. (ISO 28000 2007, 20).
Johdon sitoutuminen	Kyllä. (ISO 28000 2007, 20).
Henkilöstön koulutus ja tietoisuus	Kyllä. (ISO 28000 2007, 22).
Resursointi	Kyllä. (ISO 28000 2007, 20).
Viestintä- ja raportointisuunnitelmat sekä menettelyt	Kyllä. (ISO 28000 2007, 22).
Hallintajärjestelmän dokumentointi- ja dokumenttien hallintajärjestelmä	Kyllä. (ISO 28000 2007, 22, 28).
Suunnitelmat ja menettelytavat valmiuden ja toiminnan varmistamiseksi, turvallisuuden palauttamiseksi hätätilanteissa	Kyllä. (ISO 28000 2007, 24).
Poikkeamien, korjaavien ja ennaltaehkäisevien toimenpiteiden käsittely	Kyllä. (ISO 28000 2007, 26).
Tallenteiden hallinta	Kyllä. (ISO 28000 2007, 28).
Suorituskyvyn mittaaminen ja seuranta	Kyllä. (ISO 28000 2007, 26).
hallintajärjestelmän arviointi ja auditoiminen ja jatkuva parantaminen	Kyllä. (ISO 28000 2007, 28).

Taulukko 1 Vertailuanalyysin yhteenveto

4.2 Standardin asettamat rajoitteet

Soveltuvuuden arvioimiseksi ISO 28000 -standardin dokumentaatioon on kohdistettu sisällönanalyysi, jolla on pyritty tunnistamaan sellaiset piirteet, jotka rajoittaisivat poikkeamista standardin alkuperäisestä soveltamisalasta ja laajuudesta. Sisällönanalyysissa standardista on ensisijaisesti etsitty kielteisiä ilmaisuja, jotka rajoittavat standardin soveltamista alkuperäisestä soveltamisalasta. Lisäksi tekstistä on etsitty myös ehdottomia ilmaisuja, jotka joko linkittäisivät standardin toimitusketjujen turvallisuuteen tai määrittelisivät, että standardi ei täytä yleisesti hallintajärjestelmille asetettuja vaatimuksia.

Soveltamisalan kuvauksessa standardi painottaa toimitusketjuun kohdistuvaa järjestelmää, mutta linjaa kuitenkin: ”Tämä kansainvälinen standardi määrittelee turvallisuuden hallintajärjestelmän vaatimukset, mukaan lukien ne näkökohdat, jotka ovat kriittisiä toimitusketjujen turvallisuuden varmistamisen kannalta” (ISO 28000 2007, 10). ISO 28000 määrittelee myös, että standardi on käyttökelpoinen silloin, kun organisaatio haluaa vakiinnuttaa, toteuttaa, ylläpitää ja kehittää turvallisuuden hallintajärjestelmää (ISO 28000 2007, 10). Linjauksessa ei oteta kantaa lainkaan, rajoitteita asettaen, toimitusketjun turvallisuuteen.

Soveltamisalan kuvauksen lisäksi ISO 28000 -standardissa mainitaan toimitusketjuista ainoastaan ”toiminnan ohjauksen” yhteydessä, jossa se määrittelee, että ”organisaation on määriteltävä ne tarpeelliset toiminnot, joilla saavutetaan toimitusketjun turvallisuuden vaadittu taso” ja, että ”organisaation on varmistettava, että nämä aktiviteetit suoritetaan määritellyissä olosuhteissa arvioimalla mahdolliset uhkat toimitusketjun alkuosan toimintoihin ja ulottamalla valvonta pienentämään näitä vaikutuksia organisaatioon ja muihin toimitusketjun loppuosan toimijoihin” (ISO 28000 2007, 10). ISO 28000 -standardiin liittyvä, opastava standardi ISO 28004 ”*Security management systems for the supply chain – Guidelines for the implementation of ISO 28000*” ei myöskään rajaa stanrdardin soveltamista pelkästään toimitusketjujen turvallisuuteen. Se jopa linjaa, että hallintajärjestelmän tavoitteita ja päämääriä asetettaessa, tulisi huomioida sekä laaja-alaiset yritysturvallisuuden tavoitteet että toimitusketjujen turvallisuuteen liittyvät tavoitteet ja päämäärät (ISO 28004, 18). ISO 28000 ja ISO 28004 –standardeihin kohdistetun sisällönanalyysin perusteella voidaan todeta, että toimitusketjuihin painottuva soveltamisala ei sulje pois standardin soveltamista kokonaisvaltaisen turvallisuuden hallintajärjestelmän pohjaksi.

4.3 ISO 28000 asiantuntijan näkökulmasta

Tutkijan tekemien johtopäätösten tueksi tutkimukseen on haluttu tuoda myös ulkopuolisen asiantuntijan näkemys ISO 28000 –standardin soveltumisesta haluttuun tarkoitukseen. Yrityksen laatupäällikön haastattelun yhteydessä laatupäällikköä on pyydetty johtamis- ja hallintajärjestelmiin perehtyneenä henkilönä arvioimaan, sisältäisikö ISO 28000 kaikki hallintajärjestelmille oleelliset elementit ja piirteet.

Arvioinnin perustaksi asetettiin koodaamisen ja teemoittelun tuloksena rakennettu ISO 28000 -standardin erittely (ks. luku 4.1), josta voidaan todeta standardin asettamat vaatimukset sekä arvioida hallintajärjestelmien välisiä vastaavuuksia. Lisäksi arvioinnissa vertailtiin standardin vaatimuksia Yrityksen laatu- ja johtamisjärjestelmään, joka sisältää hallintajärjestelmien velvoittamana sekä käytännön tuomaan kokemukseen perustuen kaikki hallintajärjestelmän elementit.

Asiantuntijan näkemyksen mukaan standardin lähes yhtenevä rakenne laadunhallinta ISO 9001-standardin ja ympäristönhallinta ISO 14001-standardin kanssa tukee mahdollisuutta soveltaa ISO 28000 -standardia kokonaisvaltaiseksi hallintajärjestelmäksi. Laatupäällikön käsityksen mukaan, vertailtaessa Yrityksen johtamisjärjestelmään, ISO 28000 -standardin mukainen hallintajärjestelmä sisältää kaikki johtamisjärjestelmälle oleelliset elementit ja piirteet (Rantala 2014).

4.4 ISO 28000 ja kokonaisvaltainen turvallisuuden hallinta

Sisällönanalyysistä, vertailuanalyysistä ja haastattelusta saatujen tulosten perusteella voidaan todeta, että ISO 28000 sisältää järjestelmätasolla kaikki johtamis- ja hallintajärjestelmille oleelliset elementit. Voidaan myös todeta, että toimitusketjuihin kohdistuva painoarvo ei ole rajoittava tekijä standardin soveltamisessa laajempaan kontekstiin. Standardin alkuperäisen soveltamisalan ollessa toimitusketjun turvallisuudessa, ei toimitusketjun näkökohtia voitane kuitenkaan sivuuttaa, mikäli standardille haetaan organisaatiossa sertifiointia.

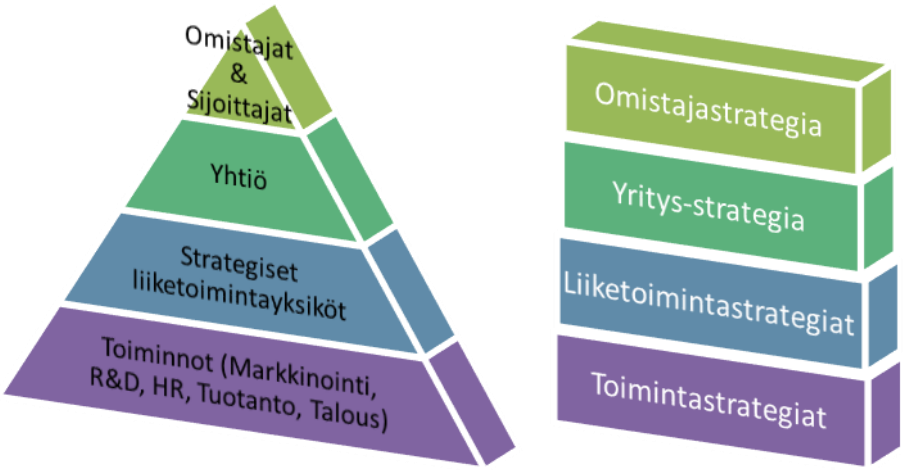
5 Vacon Oyj:n linjaukset turvallisuuden hallinnalle

ISO 28000 –standardin soveltuvuutta Yrityksen kokonaisvaltaisen turvallisuuden hallintajärjestelmän pohjaksi arvioitiin haastattelemalla Yrityksen johtoryhmää (VEMT, Vacon Executive Management Team) sekä Yrityksen laatupäällikköä. Johtoryhmän haastattelussa käsiteltiin johdon roolin kannalta oleellisia kysymyksiä, johtamiseen, vastuisiin ja resursointiin liittyen. Haastattelulla pyrittiin asettamaan turvallisuuden hallinnalle suuret linjaukset, jotka kuitenkin vaikuttaisivat olennaisesti ISO 28000 –standardin soveltuvuuteen: onko Yritys johtoryhmineen valmis sitoutumaan turvallisuuden hallintaan, nähdäänkö se osana koko organisaation toimintaa vai kenties rajattuna yhteen operatiiviseen toimintoon ja onko Yritys valmis luomaan tarvittavat resurssit ja prosessit. Haastattelukysymykset tuloksineen on purettu jäljempänä alaluvuissa. Haastattelut johtopäätöksineen kootaan jäljempänä luvussa 5.

5.1 Johtoryhmän asettama tahtotila

Johtoryhmän haastatteluun sisältyi alustus turvallisuuden hallintaan ja hallintajärjestelmästandardin vaatimuksiin, jotta kohderyhmän oli mahdollista liittää haastattelu tutkimuksen kannalta oleelliseen kontekstiin. Tutkimuksesta irrallisena hyötynä tutkimushaastattelulla ja sen alustuksella saavutettiin ensimmäinen aste johdon sitoutumisessa turvallisuuden hallintaan; Yrityksen johto on se elin, joka sysäsi hallintajärjestelmän tavoitteineen, päämäärineen ja suurine linjauksineen alkuun. Tekijänoikeudellisista syistä johtuen kaupalliseen aineistoon pohjautuvaa alustukseen käytettyä materiaalia ei käsitellä tässä raportissa.

ISO 28000 –standardi painottaa johdon sitoutumista turvallisuuden hallintaan. Haastattelun ensimmäisellä kysymyksellä haluttiin kartoittaa, miten laaja turvallisuuden hallintajärjestelmän tulisi Yrityksen johdon näkemyksen mukaan olla sekä organisaation ja prosessien osalta että strategisella tasolla. Mikäli johto määrittelisi turvallisuuden operatiivisen tason toiminnaksi tai rajoittuen yhteen toimintoon, joka ei asettaisi organisaation johdolle velvoitteita ja vastuita, ISO 28000 –standardi ei soveltuisi Yrityksen hallintajärjestelmän rungoksi. Kysymys asetettiin seuraavasti: ”Millä eri organisaation tasoilla yritysturvallisuutta tulisi mielestänne harjoittaa?”. Lisäksi kysymystä havainnollistettiin oheisella kuvalla (kuva 3 Yritystoiminnan strategiset tasot), jossa eritellään liiketoiminnan strategisia tasoja.



Kuva 1 Yritystoiminnan strategiset tasot (LogiSec Oy 2014).

Vastaajat olivat asetetun kysymyksen osalta yksimielisiä. Turvallisuuden hallinnan tulisi kattaa yhtiön koko globaalin organisaation toimintoineen ja prosesseineen, ylimmästä johdosta aina linjaorganisaation yksittäiseen työntekijään. Myös omistajaohjauksella todettiin olevan vaikutus turvallisuuden hallintaan; omistajat ja sijoittavat velvoittavat turvaamaan Yrityksen kilpailukyvyn. (VEMT 2014.)

Kysymyksellä kaksi, ”Mille seuraavista yritysturvallisuuden osa-alueista antaisitte eniten painoarvo?”, haluttiin selvittää johtoryhmän päämääriä ja tavoitteita sekä painopisteitä turvallisuuden suhteen. Mikäli johtoryhmä olisi eritoten painottanut tieto- tai työturvallisuutta, olisi tämä vaikuttanut ISO 28000 –standardin sovellettavuuteen ihanteellisena viitekehyksenä (vrt. ISO 27001 ja OHSAS 18001). Kysymystä havainnollistettiin kuvan 3, ”Yritysturvallisuuden osa-alueet”, avulla, jossa on eritelty yritysturvallisuuteen liittyvät suojattavat arvot sekä yksittäiset turvallisuuden osa-alueet.

Kuva 2 Yritysturvallisuuden osa-alueet (Elinkeinoelämän keskusliitto 2013).

Johtoryhmän mukaan Yritys haluaa valmistajana ensisijaisesti painottaa tuotannon ja toiminnan turvallisuutta (mukaan lukien logistiikan turvallisuus). Toiminnan katkeaminen tai häiriytyminen tuottaisi Yritykselle mittavia rahallisia tappioita sekä sillä olisi mahdollisesti negatiivisia vaikutuksia Yrityksen maineeseen. Toiseksi tärkeimmäksi osa-alueeksi katsottiin tietoturvallisuus, joka vaikuttaa kaikkiin Yrityksen suojattaviin arvoihin joko suoraan tai epäsuorasti. Työturvallisuus on Yritykselle itseisarvo, jota ei voida kokonaisuutena ohittaa missään tilanteessa. Kuitenkin puhtaasti toiminnan jatkuvuuden kannalta työturvallisuutta ei katsottu tärkeimmäksi osa-alueeksi. (VEMT 2014.)

Kysymyksellä kolme, ”Sisäinen turvallisuus vai ulkoistaminen? Lisäkysymys: Tulisiko turvallisuuden olla osa johtamisjärjestelmää?”, haluttiin kartoittaa tahtotilaa turvallisuuden hallintajärjestelmän rakenteen suhteen, prosessinäkökulmasta. Pyrkimyksenä oli selvittää, nähdäänkö turvallisuus muusta liiketoiminnasta irrallisena, mahdollisesti ulkoistettavana tukitoimintona vai oleellisena osana Yrityksen johtamisjärjestelmiä. Kysymyksellä oli vaikutus myös jäljempänä pidettyyn laatupäällikön haastatteluun, ISO 28000 –standardin soveltuvuuden selvittämisessä osaksi laatu- ja johtamisjärjestelmiä. Mikäli johtoryhmä olisi linjannut turvallisuuden hallintajärjestelmän täysin omaksi kokonaisuudekseen, ei järjestelmäintegraation tarkastelu myöhemmässä vaiheessa olisi ollut lainkaan tarpeen, sillä ISO 28000 -standardi olisi voitu rakentaa omaksi kokonaisuudekseen ilman rajoittavia suhteita muihin järjestelmiin.

Johtoryhmän mukaan turvallisuuden hallintajärjestelmä tulisi integroida nykyisiin laatu- ja johtamisjärjestelmiin ja sen tulisi olla selkeä osa johtamista. Hallintajärjestelmän tulee kattaa sekä prosessi- että vastuunäkökulmasta kaikki organisaation tasot. Turvallisuuden hallinnan tulisi ehdottomasti lähteä Yrityksen sisältä, ylimmästä johdosta, jotta riittävä jalkautumisesta voidaan varmistua. Yrityksellä tulisi kuitenkin olla organisaation ulkopuolisia verkos-

toja, jotka tarjoaisivat hyödynnettävää vertailu- ja asiantuntijatietoa, jotta turvallisuuden ja osaamisen taso pystytään pitämään korkealla. (VEMT 2014.)

Koko organisaation kattavan hallintajärjestelmän lanseeraaminen vaatii sekä rahallisia että henkilöstöresursseja etenkin suunnittelu- ja toteutusvaiheissa. Mikäli johtoryhmä linjaisi, ettei turvallisuustyölle haluttaisi varata resursseja kuin lakisääteisten ja muiden pakollisten vaatimusten täyttämiseksi, olisi ISO 28000 –standardin mukainen hallintajärjestelmä resurssien kannalta liian raskas sovellettavaksi.

Kysymyksellä neljä, ”Onko turvallisuuden hallintaan, ennalta ehkäisevien ja korjaavien toimenpiteiden jalkauttamiseksi, varattu mielestänne riittävät resurssit?”, haluttiin kartoittaa johdon sitoutumisen lisäksi halukkuutta varata hallintajärjestelmän toteuttamiselle, ylläpidolle ja kehittämiselle riittävät resurssit (budjetointi ja työvoima).

Johtoryhmän mukaan organisaation osaamisen- ja turvallisuuden hallinnan tason tulee olla korkea ja resursseja varataan riittävästi tarpeiden mukaan jo nykyhetkellä, mutta myös tulevaisuudessa. Johtoryhmä myös arvioi, että mikäli turvallisuuden hallintajärjestelmä otetaan suunnitellussa laajuudessaan käyttöön, se maksanee itsensä takaisin turvallisuutta koskevien asiakasvaateiden kautta. (VEMT 2014.)

Kysymyksellä viisi, ”Millä seuraavista organisaatiokulttuurin tasoista haluaisitte nähdä Vaconin tulevaisuudessa?”, haluttiin kartoittaa organisaation päämääriä ja tavoitteita turvallisuuden hallinnan ja –kulttuurin kypsyystason suhteen. Kysymystä havainnollistettiin kuvan 5 ”Turvallisuuskulttuurin kypsyysmalli” avulla. Kuvassa turvallisuuskulttuuri jaetaan neljään eri kypsyystasoon. Nollataso tarkoittaa, ettei turvallisuuden hallinnan kannalta suoriteta minkäänlaisia menettelyjä. Lakisääteinen taso kuvastaa kypsyyttä, jossa lakisääteiset ja muut ulkoiset vaatimukset tunnistetaan, mutta niiden velvoittamia menettelyjä noudatetaan varauksin ja pakon sanelemana, jolloin turvallisuus mielletään organisaation ylimääräisenä kustannustekijänä ja toiminnan jarruna. Kolmannella tasolla, ”turvallisuus”, tarkoitetaan askelta, jossa organisaatio on sitoutunut turvallisuuden hallintaan, tavoitteenaan luoda ennaltaehkäisevä, yrityksen strategiaa ja visiota tukeva, organisaatioon integroitu turvallisuuskulttuuri. Korkein taso, ”edelläkävijä” on kypsyysmallin taso, jossa organisaatio pyrkii luomaan parhaita käytänteitä ja jatkuvaa kehittämistä soveltaen turvallisuudesta itseisarvon ja kilpailuvaltin osaksi organisaation toimintaa, joka koetaan toiminnan hidastajan sijaan toiminnan mahdollistajana.

Yrityksen tulisi asettaa päämääränsä ja tavoitteensa vähintään toiseksi korkeimmalle tasolle, jotta ISO 28000 -hallintajärjestelmän rakentaminen olisi perusteltua ja mielekästä. Mikäli organisaatio asettaisi tavoitteensa tätä tasoa alemmas, olisi standardinmukaisen hallintajärjestelmän luominen ja toteuttaminen ylimitoitettua tavoitteisiin ja päämääriin nähden.

Kuva 3 Turvallisuuskulttuurin kypsyysmalli (LogiSec Oy 2014).

Johtoryhmän mukaan tavoiteltava taso on portaikoin kolmas, ”turvallisuus”. Tämä taso vastaa Yrityksen ja sen sidosryhmien vaateisiin. Turvallisuudessa halutaan painottaa ennaltaehkäisevää kulttuuria ja nolla-virheen periaatetta. Yritykseen kohdistuvat riskit tulee olla hallinnassa, johon tasolla kaksi ei päästä. Korkeinta tasoa ei kuitenkaan nähty tarpeellisena, sillä Yrityksen liiketoimintaideasta johtuen turvallisuutta ei koettu tekijänä, jolla saavutettaisiin kilpailuetua ja lisäarvoa Yrityksen brändiin. (VEMT 2014.)

Viimeisellä kysymyksellä 6, ” Minkälaisia turvallisuuteen liittyviä raportteja Yrityksen johto haluaisi käsitellä? Lisäkysymys: Minkälaisen viestin Yrityksen johto haluaa antaa organisaatiolle/asiakkaille/kumppaneille/sijoittajille turvallisuusasioista?” haluttiin kartoittaan sekä painottaa johdon sitoutumisen tasoa (mm. johdon katselmus ja turvallisuusasioista viestiminen) varsinaiseen turvallisuustyöhön. Johdon tulisi olla tietoinen liiketoiminnan kannalta oleellisista turvallisuusriskeistä sekä osoittaa sitoutumistaan turvallisuuteen osallistumalla ja viestimällä turvallisuuden hallinnan periaatteista ja menettelyistä.

Pääkysymykseen ei saatu yksiselitteistä vastausta. Johtoryhmä kuitenkin totesi, että sen on oltava tietoinen sekä liiketoimintaan liittyvistä että Yrityksen ulkopuolisista uhista ja riskeistä, sillä riskejä turvallisuuden suhteen ei haluta ottaa missään tilanteessa. Viestinnän suhteen johtoryhmä linjasi, että turvallisuuden hallinta tulee integroida näkyvästi organisaation toimintaan. Turvallisuusjohtajan tulee selkeästi viestiä toiminnan kautta, että turvallisuustyö on

osa agendaa ja jokapäiväistä toimintaa. Myös sidosryhmille halutaan viestiä, että Vacon on turvallinen kumppani. (VEMT 2014.)

5.2 Turvallisuuden hallinta osana Yrityksen laatu- ja johtamisjärjestelmää

ISO 28000 –standardin soveltuvuutta Yrityksen käyttöön arvioitiin haastattelemalla ulkopuolista asiantuntijaa, Yrityksen laatupäällikköä Petri Rantalaa, joka vastaa Yrityksen laatu- ja johtamisjärjestelmän koordinoinnista. Haastattelun runkona käytettiin tämän tutkimuksen aikana syntynyttä ISO 28000 -vaatimuslistaa (ks. s.41), jota pyydettiin vertaamaan Yrityksen nykyiseen johtamisjärjestelmään ja arvioimaan standardin soveltuvuutta osaksi järjestelmää. Haastateltavalle annettiin myös mahdollisuus vapaaseen sanaan.

Rantalan (2014) mukaan ISO-perheeseen kuuluvan standardin implementoiminen osaksi Yrityksen johtamisjärjestelmää olisi mielekästä, sillä nykyinen laatu- ja johtamisjärjestelmä perustuu ISO 9001-, ISO 14001- ja OHSAS 18001 standardeihin. Laatupäällikön mukaan Yrityksessä tavoitellaan täysin harmonisoitua ja konsolidoitua johtamisjärjestelmää, jossa kaikki prosessit kuten laatu, ympäristö ja turvallisuus, olisivat integroituna samaan järjestelmää. ISO 28000 sopisi rakenteensa ansiosta hyvin osaksi ISO- ja OHSAS-standardeihin perustuvaa johtamisjärjestelmää.

ISO 28000 -standardin vaatimusten tarkastelussa Rantala (2014) painottaa ISO-standardien hyvin pitkälle yhtenevää rakennetta, joka luo mahdollisuuksia standardin menestyksekkääksi soveltamiseksi. Kaikki haastattelussa käsitellyistä standardin osa-alueista olisivat Rantalan mukaan sovellettavissa osaksi Yrityksen nykyistä ja tulevaa järjestelmää. Jokainen olemassa olevanjohtamisjärjestelmän elementti pitäisi kuitenkin arvioida, suunnitella ja toteuttaa uudelleen, jotta ISO 28000 -standardin kannalta vaadittavat näkökulmat voitaisiin integroida osaksi järjestelmää. (Rantala 2014.)

Yhteenvetona laatupäällikkö toteaa, että standardi olisi erittäin hyvä viitekehys turvallisuuden hallintajärjestelmän uudelleen organisoimiseksi ja toteuttamiseksi. (Rantala 2014.) Rantalan (2014) mukaan hallintajärjestelmän toteuttaminen vaatii kuitenkin paljon resursointia ja ennen kaikkea osaamista, sillä standardi ei anna yksiselitteisiä vaatimuksia tai ratkaisuja osa-alueiden toteuttamiseksi. Isoa osaa olemassa olevasta hallintajärjestelmästä voitaisiin kuitenkin hyödyntää sellaisenaan.

6 ISO 28000 soveltuvuus Vacon Oyj:n turvallisuuden hallintajärjestelmäksi

Tutkija esittää luvussa 3.5, että ISO 28000 -standardia voidaan soveltaa kokonaisvaltaiseksi turvallisuuden hallintajärjestelmäksi. Tutkimuksena toisena tavoitteena oli arvioida saatujen

tutkimustuloksiin pohjautuen, soveltuisiko standardi kokonaisvaltaisena turvallisuuden hallintajärjestelmän runkona Yrityksen käyttöön. Johtoryhmän haastattelun perusteella (ks. luku 5.1) ISO 28000 soveltuu Yrityksen käyttöön. Haastattelun tarkoituksena tutkimuksen kannalta oli ensiarvoisesti kartoittaa Yrityksen johdon tahtotilaa sekä tavoiteltavan turvallisuuden hallinnan tason suhteen että tarvittavan sitoutumiseen ja resurssien varaamiseen. Yhteenvetona johtoryhmän haastattelusta voidaan todeta, että johtoryhmä:

a) haluaa sitoutua turvallisuuden hallintaan
b) tavoittelee hyvää turvallisuuskulttuuria
c) on valmis varaamaan turvallisuuden hallintaan riittävät resurssit.

Kuten Kerkokin (2001, 26) esittää, edellä listatut seikat ovat olennaisia turvallisuuden hallinnassa. ISO 28000 vaatii johdon sitoutumista ja riittävien resurssien varaamista, joka osoittaa, että johtoryhmän asettamat linjaukset ovat yhdenmukaisia standardin velvoitteiden kanssa. (ISO 28000 2007, 14-20). Mikäli Yrityksen johto ei ole valmis sitoutumaan ja varaamaan turvallisuuden hallintaan riittäviä resursseja, standardin mukaisia menettelyjä ei voida luoda toimiviksi. Mikäli johtoryhmä olisi linjannut, että riittävä turvallisuuskulttuurin taso saavutetaan lakisääteiset velvoitteet täyttämällä, ei ISO 28000 -standardin soveltaminen organisaatioon olisi kustannusten ja tehokkuuden puitteissa perusteltavissa. Soveltuvuutta tukee osaltaan myös johtoryhmän linjaus turvallisuustyön painopisteen asettamisesta tuotannon ja toiminnan turvallisuudelle (mukaan lukien toimitusketjujen turvallisuus). Mikäli johtoryhmä olisi nostanut tärkeimmäksi osa-alueeksi esimerkiksi tietoturvallisuuden, olisi ISO 27001-standardin mukainen järjestelmä ollut enemmän perusteltua.

Myös Yrityksen laatupäällikön haastatteluun (ks. luku 5.2) perustuen voidaan todeta, että standardi soveltuisi Yrityksen käyttöön. Rantalan (2014) mukaan kaikki ISO 28000 -standardin mukaiset menettelyt olisivat sovellettavissa osaksi Yrityksen nykyistä ja tulevaa johtamisjärjestelmää, joka perustuu ISO 9001, OHSAS 18001 – ja 14001-standardeihin. Kuten vertailuanalyysissä (ks. luku 4.1 & liite 1) todetaan, ISO 28000 on lähestulkoon kokonaisuudessaan yhdenmukainen edellä mainittujen viitekehysten kanssa. Suurimman pesäeron se luo toiminnan ohjauksen ja jalkauttamisen suhteen, jotka edellyttävät turvallisuuden hallintaohjelmien luomista tarvittaville yritysturvallisuuden osa-alueille. Rantala (2014) toteaa haastattelun yhteenvetona, että ISO-perheen standardi olisi erittäin mielekäs viitekehys turvallisuuden hallintajärjestelmän uudelleen organisoimiseksi ja toteuttamiseksi.

Varsinaisten tutkimusmenetelmin tuotettujen tulosten lisäksi tutkija esittää omaan subjektiiviseen näkemykseensä perustuvia väitteitä standardin soveltuvuudesta. Tutkijan näkemyksen mukaan standardi sopisi Yrityksen käyttöön, koska:

a) ISO 28000 perustuu ISO 14001-standardin mukaiseen, riskeihin perustuvaan lähestymistapaan, joskaan se ei poissulje prosessimuotoisen hallintajärjes-

telmän (ISO 9001) soveltamista turvallisuuden hallintajärjestelmän perustaksi (ISO 28000 2007, 8.)

b) Yrityksen tavoittelema AEO-status perustuu tietyiltä osin ISO 28000 -standardin menettelyihin
c) ISO 28000 ei sulje pois muiden standardien käyttöä, vaan sitä olisi mahdollista soveltaa ns. ylätason järjestelmänä, joka kokoaa kaikki turvallisuuden hallinnan osa-alueet (ja muiden standardien asettamat menettelyt) yhteen
d) määrittelyn mukaan standardi on sovellettavissa kaikenlaisiin organisaatioihin (ISO 28000 2007, 10.)
e) se ei anna tarkkoja linjauksia menettelyjen toteuttamiseksi, joka luo vapauden suorittaa tarvittavat toimenpiteet organisaatioon ja sen resursseihin istuvalla tavalla
f) standardi voisi olla sovellettavissa organisaation käyttöön myös alkuperäisen soveltamisalansa puitteissa; johtoryhmän linjauksen mukaan tuotannon ja toiminnan turvallisuus (ml. toimitusketjun turvallisuus) on tärkein yksittäinen yritysturvallisuuden osa-alue Yrityksessä.

Tutkimuksen yhteenvetona tutkija esittää tässä luvussa eritellyin perustein, että ISO 28000 –standardia voidaan soveltaa alkuperäisestä soveltamisalastaan kokonaisvaltaiseksi turvallisuuden hallintajärjestelmän rungoksi. Tutkija esittää myös, että standardi soveltuu sisältönsä ja vapaan rajaamisen johdosto Yrityksen käyttöön. Standardin valintaa Yrityksen hallintajärjestelmän rungoksi tukevat yhtymäkohdat muihin hallintajärjestelmästandardeihin ja AEO-vaatimuksiin. Tutkimustulokset johtopäätöksineen rajoittuvat kuitenkin teoriatasoon. Johtopäätösten valossa ei voida todeta järjestelmän ongelmatonta soveltamista ja integraatiota Yrityksen käyttöön.

7 Pohdinta ja aiheita jatkotutkimukseen

Tutkimus täyttää sille asetetut tavoitteet. Tuloksina todetaan, että ISO 28000 -standardi täyttää sekä kokonaisvaltaiselle hallintajärjestelmälle asetetut vaatimukset että Yrityksen turvallisuuden hallintajärjestelmälle asettamat tarpeet ja tavoitteet. Teoriaan sekä tutkimusmenetelmien toimivuuteen perustuen tutkija esittää saatuja tutkimustuloksia luotettaviksi. Tutkimustulosten tarkastelussa on kuitenkin huomioitava tulosten sovellettavuus ja yleistettävyys laajempaan ja/tai eriävään kontekstiin ainoastaan teoreettisella tasolla ja tutkimuksen rajauksen puitteissa. Kattavamman yleistyksen haasteena tutkimuksessa ovat vähäinen ja keskenään samankaltainen tapausjoukko. Tapausjoukon rajaaminen on kuitenkin perusteltua, sillä tutkimuksessa on haluttu keskittyä ainoastaan standardeihin tai standardinomaisiin turvallisuuden ja hallintajärjestelmien viitekehyksiin, turvallisuusjohtamiselle ja hallintajärjes-

telmille oleellisten elementtien jäsentämiseksi. Saatuja tuloksia ei voida täten pitää täysin soveltuvina tutkimuksessa rajatun tarkastelujoukon ulkopuolella.

Käytännön tason soveltuvuutta muuhun kuin tässä tutkimuksessa käsiteltyyn kohdeorganisaatioon ei voida todeta ilman jatkotutkimusta ja halutun kohdeorganisaation ominaisuuksien tarkastelua.

Tutkimus on prosessina onnistunut. Laadittu tutkimusstrategia osoittautui toimivaksi, eikä strategiasta poikettu tutkimuksen edetessä lainkaan. Myös suunnitellut metodit osoittautuivat tutkimuksen edetessä soveltuviksi ja valideiksi, sillä analyyseistä saadut tulokset vastaavat asetettuihin tutkimuskysymyksiin. Tulokset pystytään myös perustelemaan teoreettisesti, ilman tutkijan subjektiivista näkemystä ja tulkintaa. Toisistaan eriävien metodien mahdollistava triangulaatio lisää oleellisesti tutkimustulosten luotettavuutta, sillä tutkimuksen kohteena ollutta ISO 28000 -standardia voitiin tarkastella sekä objektiivisesti, subjektiivisesti että liittämällä se laajempaan kontekstiin.

Ensimmäisen vaiheessa saadut tulokset olivat avainasemassa tutkimuksen toisen vaiheen kannalta. Mikäli saadut tulokset olisivat osoittaneet, että ISO 28000 –standardia ei olisi sovellettavissa haluttuun tarkoitukseen, olisi tutkija esittänyt tutkimustuloksinaan yksiselitteisesti, että viitekehys ei ole sovellettavissa haluttuun tarkoitukseen. Jatkotutkimusaiheeksi olisi tällöin muodostunut Yritykseen parhaiten soveltuvan turvallisuuden hallintajärjestelmän kartoittamistyö.

Vertailuanalyysissä haasteelliseksi osoittautui AEO-viitekehys, joka vaati osittain tutkijan tulkintaa turvallisuudelle ja sen hallinnalle asetettujen vaatimusten jäsentämiseksi. Viitekehyksen tekstiaineisto ei aseta suoria tai yksiselitteisiä vaatimuksia vaan se on luonteeltaan kysyvä, joka jättää tulkinnan ja johtopäätösten tekemisen lukijalleen. Tutkija on kuitenkin toiminut kyseisin viitekehyksen asiantuntijana useassa sertifiointiprosessissa, joka mahdollisti viitekehyksen koodaamisen muihin viitekehyksiin nähden vertailukelpoiseksi.

Tutkimushaastatteluilla onnistuttiin keräämään tutkimuksen kannalta oleellinen tieto. Johtoryhmän haastattelun ulkopuolelle jäi kuitenkin jonkin verran arvokasta, syventävää tietoa, jota ei voitu analysoida. Haastattelua edeltäneen turvallisuuden hallinnan johdannon aikana esiintyi paljon arvokasta keskustelua, jota ei tutkimuksen ulkopuolisena kokonaisuutena nauhoitettu lainkaan. Tästä johtuen johdannon keskusteluista saatiin kirjattua ainoastaan vajavaisia muistiinpanoja. Tilaisuuden haastatteluosiossa kuitenkin saatiin kerättyä tutkimuksen kannalta tarvittava tieto.

Tutkimuksen tulokset esitettiin Yrityksen edustajille sekä koottuna esityksenä että raportin muodossa. Esityksen yhteydessä kerättiin suullinen palaute tutkimusprosessin onnistumisesta ja tutkimustulosten sovellettavuudesta. Yrityksen edustajien mukaan tutkimus vastaa asetettuihin tutkimuskysymyksiin riittävällä tarkkuudella. Tutkimuksen tuloksia aiotaan soveltaa turvallisuuden hallinnan kehittämiseksi, ottamalla ISO 28000 -standardi hallintajärjestelmän rungoksi kehitystyössä. Yritys pyrkii standardin asettamien vaatimusten mukaiseen tapaan toimia, joka saattaa johtaa tulevaisuudessa myös sertifioitumiseen. Yrityksen mukaan suurin hyöty saavutettiin kuitenkin itse tutkimusprosessin aikana. Prosessi aktivoi johto- ja laaturyhmää turvallisuuden hallinnan edistämiseksi sekä lisäsi tietoisuutta ja antoi vastauksia liiketoiminnan kannalta oleellisiin turvallisuutta käsitteleviin kysymyksiin. Erityismaininta haluttiin osoittaa osallistavalle ja aktiiviselle tutkimusotteelle, joka toimi valmistelevana työnä aloitettavalle turvalllisuuden kehittämishankkeelle.

Tämän tutkimuksessa ei voida todeta ISO 28000 -standardiin perustuvan kokonaisvaltaisen turvallisuuden hallintajärjestelmän toimivuutta käytännössä. Tutkija esittää jatkotutkimusaiheeksi toiminallista tutkimusta, jossa rakennetaan standardiin perustuva turvalisuuden hallintajärjestelmä. Hallintajärjestelmän toimivuutta tulisi myös mitata käytännössä.

Lähteet

Kirjalliset lähteet:

Anttila, P. 2006. Tutkiva toiminta ja ilmaisu, teos, tekeminen. 2.painos. Hamina: Akatiimi.

Bamberg, J., Jokinen, P. & Laine, M. 2007. Tapaustutkimuksen taito. Helsinki: Yliopistopaino

Euroopan komissio. 2012. Valtuutetut talouden toimijat - Suuntaviivat.

Halibozek, E. & Kovacich, G. 2003 The manager's handbook for corporate security: establishing and managing a successful assets protection program. USA: Butterworth–Heinemann.

Hirsjärvi, S. & Hurme, H. 2009. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15.–17. painos. Helsinki: Tammi.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2010. Johda riskejä. Käytännön opas yrityksen riskienhallintaan. Pössneck: Tammi

ISO 9000, 2005. SFS-EN ISO 9000. Laadunhallintajärjestelmät. Perusteet ja sanasto. 2.painos. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 9001, 2008. SFS-EN ISO 9001. Laadunhallintajärjestelmät. Vaatimukset. 4.painos. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 27000. 2005. SFS-ISO/IEC 27000. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 27001. 2006. ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 28000. 2007. SFS-ISO 28000. Toimitusketjun turvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS.

ISO 28001. 2007. Security management systems for the supply chain. Best practices for implementing supply chain security assessments and plans. Requirements and guidance. Geneve: International Organization for Standardization (ISO).

ISO 28004. 2007. Security management systems for the supply chain – Guidelines for the implementation of ISO 28000. Geneve: International Organization for Standardization (ISO).

ISO 31000, 2011. SFS-ISO 31000. Riskienhallinta. Periaatteet ja ohjeet. Helsinki: Suomen Standardisoimisliitto SFS.

Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus

Kunttu,T. 2012. Turvallisuusjohtamisjärjestelmien vertailu. Tutkimusraportti. Merenkulku ja logistiikka. Kotka: Kymenlaakson ammattikorkeakoulu.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Jyväskylä: Gummerus.

Levä, K. 2003. Turvallisuusjohtamisjärjestelmien toimivuus: vahvuudet ja kehityshaasteet suuronnettomuusvaarallisissa laitoksissa. Helsinki: Turvatekniikan keskus.

Liimatta, A. 2011. Venäjän kauttakulkuliikenteen turvallisuusriskit ja niiden ennaltaehkäiseminen. Opinnäytetyö. Kymeenlaakson ammattikorkeakoulu.

OHSAS 18001:fi, 2007. Työterveys- ja työturvallisuusjohtamisjärjestelmät. Vaatimukset. 3. painos. Helsinki: Suomen Standardoimisliitto SFS.

Puolustusministeriö. 2011. Kansallinen turvallisuusauditointikriteeristö (KATAKRI). Versio II. Helsinki: Puolustusministeriö.

Stenberg, I. 2014. Turvallisuusjohtamisjärjestelmä Maapuolustuskorkeakoulussa. Opinnäytetyö. Leppävaara: Laurea-ammattikorkeakoulu.

Sähköiset lähteet:

Elinkeinoelämän keskusliitto. 2013. Yritysturvallisuuden osa-alueet. Viitattu 12.8.2014. http://www.ek.fi/ek/fi/tyomarkkinat_ym/Yritysturvallisuus/Kuvat/Esitys_turvallisuusjohtaminen.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Verkkojulkaisu. Viitattu 25.8.2014
http://www.fsd.uta.fi/menetelmaopetus/kvali/index.html

Suomen standardisoimisliitto 2014a. Mikä on standardi?. Viitattu 27.9.2014
http://www.sfs.fi/usein_kysyttya#Mikonstandardi

Suomen standardisoimisliitto 2014b. Hallintajärjestelmästandardit ja niiden yhdistetty käyttö. Viitattu 27.9.2014
http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/ohsas_18001_tyoterveys-_ja_tyoturvallisuusjohtaminen/hallintajarjestelma-standardien_yhdistetty_kaytto

Tulli. 2014. AEO – valtuutettu taloudellinen toimija. Viitattu 29.9.2014.
http://www.tulli.fi/fi/yrityksille/asiakkaana_tullissa/AEO/index.jsp

Tullihallitus. 2008. Vähimmäisvaatimukset AEO-todistusta hakevalla yritykselle. Verkkojulkaisu. Viitattu 12.9.2014.
http://www.tulli.fi/fi/yrityksille/asiakkaana_tullissa/AEO/kiinnostuitko/AEOvahimmaisvaatimukset.pdf

Haastattelut ja julkaisemattomat lähteet:

LogiSec Oy. Johdatus turvallisuuden hallintaan. Koulutusmateriaali. 19.8.2014. Vantaa

Rantala, P. Laatupäällikön haastattelu. 15.9.2014. Vacon Oyj. Vantaa

VEMT (Vacon Executive Management Team). Johtoryhmän haastattelu. 20.8.2014. Vacon Oyj. Vantaa

Kuvat

Kuviot

Taulukot

Liitteet

Liite 1 Vertailuanalyysi: Viitekehysten väliset vastaavuudet

Oheisissa taulukoissa on kuvattu tässä tutkimuksessa käsiteltyjen viitekehysten välisiä vastaavuuksia, hallintajärjestelmille oleellisten elementtien osalta.

Politiikka		**Lähdeviite**
AEO	Turvallisuuspolitiikka	Vähimmäisvaatimukset AEO-todistusta hakevalle yritykselle (Tullihallitus 2008, 3.)
KATAKRI	Turvallisuuspolitiikka	KATAKRI A101.0 –A108.0
OHSAS 18001	TTT-politiikka	OHSAS 18001:2007, luku 4.2
ISO 9001	Laatupolitiikka	ISO 9001:2008, luku 5.3
ISO 14001	Ympäristöpolitiikka	ISO 14001:2004, luku 4.2
ISO 27001	Tietoturvallisuuspolitiikka	ISO 27001:2006, luku 4.2.1
ISO 28000	Turvallisuuden hallintapolitiikka	ISO 28000:2007, luku 4.2
ISO 31000	Riskienhallintapolitikka	ISO 31000:2009, luku 4.3.2

Taulukko 1 Viitekehysten väliset vastaavuudet: Politiikka

Riskienarviointi		**Lähdeviite**
AEO	Taloudellisen toimijan tekemä itsearviointi	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.1
KATAKRI	Riskien tunnistus, arviointi ja kontrollit	KATAKRI A400
OHSAS 18001	Vaaran tunnistaminen, riskin arviointi ja hallintatoimenpiteiden määrittäminen	OHSAS 18001:2007, luku 4.3.1
ISO 9001	Ei vaatimuksia (Tuotteeseen liittyvien vaatimusten määrittäminen)	ISO 9001:2008, luku 7.2.1
ISO 14001	Ympäristönäkökohdat	ISO 14001:2004, luku 4.3.1
ISO 27001	Ei vaatimuksia (HUOM. Tietoturvallisuusriskien arviointi osana prosessia, ei hallintajärjestelmän perustana)	ISO 27001:2006, luku 4.2.1
ISO 28000	Turvallisuusriskien arviointi	ISO 28000:2007, luku 4.3.1
ISO 31000	Organisaation ja toimintaympäristön ymmärtäminen	ISO 31000:2009, luku 4.3.1

Taulukko 2 Viitekehysten väliset vastaavuudet: Riskienarviointi

Lakisääteiset ja ulkoiset vaatimukset		Lähdeviite
AEO	Tullivaatimusten noudattaminen Taloudellinen vakavaraisuus	AEO Suuntaviivat 2012, osa 2, luku 2.1 AEO Suuntaviivat 2012, osa 2, luku 2.4
KATAKRI	Lainsäädännön tunteminen ja soveltaminen	KATAKRI A105.0 & A105.1
OHSAS 18001	Lakisääteiset ja muut vaatimukset	OHSAS 18001:2007, luku 4.3.2
ISO 9001	Asiakaskeskeisyys Tuotteeseen liittyvien vaatimusten määrittäminen	ISO 9001:2008, luku 5.2 ISO 9001:2008, luku 7.2.1
ISO 14001	Lakisääteiset ja muut vaatimukset	ISO 14001:2004, luku 4.3.2
ISO 27001	Riskienarviointi: lakisääteiset vaatimukset Tallenteiden ohjaus: lakisääteiset vaatimukset Resurssien varaaminen: lakisääteisten ja hallinnollisten vaatimusten tunnistaminen ja osoittaminen	ISO 27001:2006, luku 4.2.1 alakohta c ISO 27001:2006, luku 4.3.3 ISO 27001:2006, luku 5.2.1 alakohta c
ISO 28000	Lakisääteiset, viranomais- ja muut turvallisuusvaatimukset	ISO 28000:2007, luku 4.3.2
ISO 31000	Organisaation ulkoinen toimintaympäristö	ISO 31000:2009, luku 4.3.1 alakohta a & 5.3.2

Taulukko 3 Viitekehysten väliset vastaavuudet: Lakisääteiset ja ulkoiset vaatimukset

Tavoiteasetanta		Lähdeviite
AEO	Visio, tehtävä ja strategia	AEO Suuntaviivat 2012, osa 1, luku 1, alakohta 4
KATAKRI	Turvallisuuden tavoitteiden määrittely	KATAKRI A300
OHSAS 18001	Päämäärät ja ohjelmat	OHSAS 18001:2007, luku 4.3.3
ISO 9001	Laatutavoitteet ja laadunhallintajärjestelmän suunnittelu	ISO 9001:2008, luvut 5.4.1-5.4.2
ISO 14001	Päämäärät, tavoitteet ja ohjelmat	ISO 14001:2004, luku 4.3.3
ISO 27001	Tietoturvallisuuden tavoitteet	ISO 27001:2006, luku 4.2.1 alakohta b
ISO 28000	Turvallisuuden hallinnan päämäärät ja tavoitteet	ISO 28000:2007, luvut 4.3.3-4.3.4
ISO 31000	Riskienhallinnan tavoitteet	ISO 31000:2009, luku 4.3.1

Taulukko 4 Viitekehysten väliset vastaavuudet: Tavoiteasetanta

Resursointi		Lähdeviite
AEO	Toimeenpanovaltuudet	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.3
KATAKRI	Resurssien suuntaaminen	KATAKRI A503.0
OHSAS 18001	Resurssit, roolit, vastuut, velvollisuudet ja valtuudet	OHSAS 18001:2007, luku 4.4.1
ISO 9001	Resurssien varaaminen	ISO 9000:2008, luku 6.1
ISO 14001	Resurssit, roolit, vastuut ja valtuudet	ISO 14001:2004, luku 4.4.1
ISO 27001	Resurssien varaaminen	ISO 27001:2006, luku 5.2.1
ISO 28000	Turvallisuuden hallinnan rakenne, valtuudet ja vastuut	ISO 28000:2007, luku 4.4.1
ISO 31000	Resurssit	ISO 31000:2009, luku 4.3.5

Taulukko 5 Viitekehysten väliset vastaavuudet: Resursointi

Organisaation vastuut ja valtuudet		Lähdeviite
AEO	Sisäinen järjestely (organisaatio)	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.3
KATAKRI	Turvallisuusorganisaatio ja vastuut	KATAKRI A500
OHSAS 18001	Resurssit, roolit, vastuut, velvollisuudet ja valtuudet	OHSAS 18001:2007, luku 4.4.1
ISO 9001	Vastuut ja valtuudet	ISO 9001:2008, luku 5.5.1
ISO 14001	Resurssit, roolit, vastuut ja valtuudet	ISO 14001:2004, luku 4.4.1
ISO 27001	Tietoturvallisuuden hallintajärjestelmän toteuttaminen ja käyttäminen: vastuiden määrittäminen	ISO 27001:2006, luku 4.2.2 alakohta 2 & 5.1 alakohta c
ISO 28000	Turvallisuuden hallinnan rakenne, valtuudet ja vastuut	ISO 28000:2007, luku 4.4.1
ISO 31000	Vastuut ja velvollisuudet	ISO 31000:2009, 4.3.3

Taulukko 6 Viitekehysten väliset vastaavuudet: Organisaation vastuut ja valtuudet

Johdon sitoutuminen		Lähdeviite
AEO	N/A (Suositus johtotason henkilön nimeämiseksi AEO-vastaavaksi)	AEO Suuntaviivat 2012, osa 1, luku 1, alakohta 4
KATAKRI	Johdon hyväksyntä turvallisuuspolitiikalle Johdon tuki turvallisuudesta vastaavalle henkilölle Johdon sitoutuminen turvallisuustavoitteisiin ja jatkuvaan parantamiseen	KATAKRI A101.0 KATAKRI A504.0 & A505.0 KATAKRI 506.0
OHSAS 18001	Resurssit, roolit, vastuut ja valtuudet Johdon katselmus	ISO 14001:2004, luku 4.4.1 ISO 14001:2004, luku 4.6
ISO 9001	Johdon sitoutuminen Johdon edustaja Johdon katselmus Jatkuva parantaminen	ISO 9001:2008, luku 5.1 ISO 9001:2008, luku 5.5.2 ISO 9001:2008, luvut 5.6-5.6.3 ISO 9001:2008, luku 8.5.1
ISO 14001	Johdon katselmus	ISO 14001:2004, luku 4.6
ISO 27001	Johdon sitoutuminen	ISO 27001:2006, luku 5.1
ISO 28000	Turvallisuuden hallinnan rakenne, valtuudet ja vastuut Johdon katselmus ja jatkuva parantaminen	ISO 28000:2007, luku 4.4.1 ISO 28000:2007, luku 4.6
ISO 31000	Vastuut ja valtuudet: Johdon rooli	ISO 31000:2009, luku 4.2

Taulukko 7 Viitekehysten väliset vastaavuudet: Johdon sitoutuminen

Toiminnan ohjaus		Lähdeviite
AEO	Liiketoiminnan hallinta	AEO Suuntaviivat 2012, osa 1, luku 1, alakohta 4
KATAKRI	Turvallisuuden vuotuinen toimintaohjelma	KATAKRI A201.0-A203.0
OHSAS 18001	Toiminnan ohjaus	OHSAS 18001:2007, luku 4.4.6
ISO 9001	Tuotteen toteuttamisen suunnittelu	ISO 9001:2008, luvut 7.1-7.5.5
ISO 14001	Toiminnan ohjaus	ISO 14001:2004, luku 4.4.6
ISO 27001	Tietoturvallisuuden hallintajärjestelmän toteuttaminen ja käyttäminen	ISO 27001:2006, luku 4.2.2
ISO 28000	Toiminnan ohjaus Turvallisuuden hallinnan ohjelmat	ISO 28000:2007, luku 4.4.6 ISO 28000:2007, luku 4.3.5
ISO 31000	Sisällyttäminen organisaation prosesseihin	ISO 31000:2009, luku 4.3.4

Taulukko 8 Viitekehysten väliset vastaavuudet: Toiminnan ohjaus

Pätevyys, koulutus ja tietoisuus		**Lähdeviite**
AEO	Turvatietoisuusohjelmat	AEO Suuntaviivat 2012, osa 2, luku 2.4 alakohta G
KATAKRI	Tuvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen	KATAKRI A800
OHSAS 18001	Pätevyys, koulutus ja tietoisuus	OHSAS 18001:2007, luku 4.4.2
ISO 9001	Pätevyys, koulutus ja tietoisuus	ISO 9001:2008, luku 6.2.2
ISO 14001	Pätevyys, koulutus ja tietoisuus	ISO 14001:2004, luku 4.4.2
ISO 27001	Koulutus, tietoisuus ja pätevyys	ISO 27001:2006, luku 5.2.2
ISO 28000	Pätevyys, koulutus ja tietoisuus	ISO 28000:2007, luku 4.4.2
ISO 31000	Riskienhallinnan puitteiden toteuttaminen	ISO 31000:2009, luku 4.4.1

Taulukko 9 Viitekehysten väliset vastaavuudet: Pätevyys, koulutus ja tietoisuus

Viestintä		**Lähdeviite**
AEO	Turvallisuutta vaarantavien tilanteiden raportointi ja turvakäytäntöjen tiedottaminen	AEO Suuntaviivat 2012, liite 1. AEO-itsearviointilomakkeen selittävät huomautukset, luku 5.1.5
KATAKRI	Turvallisuuspolitiikan ja –menettelyiden tiedottaminen henkilöstölle	KATAKRI A106.0
OHSAS 18001	Viestintä, osallistuminen ja yhteistoiminta	OHSAS 18001:2007, luku 4.4.3
ISO 9001	Sisäinen viestintä Viestintä asiakkaan kanssa	ISO 9001:2008, luku 5.5.3 ISO 9001:2008, luku 7.2.3
ISO 14001	Viestintä	ISO 14001:2004, luku 4.4.3
ISO 27001	Ei vaatimuksia	
ISO 28000	Viestintä	ISO 28000:2007, luku 4.4.3
ISO 31000	Viestintä ja tiedonvaihto	ISO 31000:2009, luku 5.2

Taulukko 10 Viitekehysten väliset vastaavuudet: Viestintä

Dokumentointi		Lähdeviite
AEO	Turvallisuusmenettelyiden dokumentointi (Turvallisuussuunnitelma)	AEO Suuntaviivat 2012, liite 1. AEO-itsearviointilomakkeen selittävät huomautukset, luku 5
KATAKRI	Turvallisuusdokumentaatio ja sen hallinta	KATAKRI A700
OHSAS 18001	TTT-järjestelmän dokumentointi	OHSAS 18001:2007, luku 4.4.4
ISO 9001	Yleiset vaatimukset Laatukäsikirja	ISO 9001:2008, luku 4.2.1 ISO 9001:2008, luku 4.2.2
ISO 14001	Dokumentointi	ISO 14001:2004, luku 4.4.4
ISO 27001	Tietoturvallisuuden hallintajärjestelmän dokumentointi	ISO 27001:2006, luku 4.3.1
ISO 28000	Turvallisuuden hallintajärjestelmän dokumentointi	ISO 28000:2007, luku 4.4.4
ISO 31000	Dokumentoidut prosessit ja menettelyt (resursointi)	ISO 31000:2009, luku 4.3.5

Taulukko 11 Viitekehysten väliset vastaavuudet: Politiikka

Asiakirjojen ja tallenteiden hallinta		Lähdeviite
AEO	N/A	
KATAKRI	Turvallisuusdokumentaatio ja sen hallinta	KATAKRI A701.0
OHSAS 18001	Asiakirjojen hallinta Tallenteiden hallinta	OHSAS 18001:2007, luku 4.4.5 OHSAS 18001:2007, luku 4.5.4
ISO 9001	Asiakirjojen hallinta Tallenteiden hallinta	ISO 9001:2008, luku 4.2.3 ISO 9001:2008, luku 4.2.4
ISO 14001	Asiakirjojen hallinta Tallenteiden hallinta	ISO 14001:2004, luku 4.4.5 ISO 14001:2004, luku 4.4.5
ISO 27001	Asiakirjojen ohjaus Tallenteiden ohjaus	ISO 27001:2006, luku 4.3.2 ISO 27001:2006, luku 4.3.3
ISO 28000	Asiakirjojen ja tiedon hallinta Tallenteiden hallinta	ISO 28000:2007, luku 4.4.5 ISO 28000:2007, luku 4.5.4
ISO 31000	Riskienhallintaprosessin tallenteet	ISO 31000:2009, luku 5.7

Taulukko 12 Viitekehysten väliset vastaavuudet: Asiakirjojen ja tallenteiden hallinta

Toiminta poikkeustilanteissa		Lähdeviite
AEO	N/A (Turvallisuussuunnitelma), Tietoturva: jatkuvuus- ja palautumissuunnitelma	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.1 & 3.8.2
KATAKRI	Jatkuvuuden hallintamenettely Vastuut poikkeus- ja kriisitilanteissa Tietoturvapoikkeamatilanteiden hallinta	KATARKI A601.0 KATARKI A602.0 & A603.0 A410.0
OHSAS 18001	Valmius ja toiminta hätätilanteissa	OHSAS 18001:2007, luku 4.4.7
ISO 9001	Poikkeavan tuotteen ohjaus	ISO 9001:2008, luku 8.3
ISO 14001	Valmius ja toiminta hätätilanteissa	ISO 14001:2004, luku 4.4.7
ISO 27001	Ei vaatimuksia	
ISO 28000	Valmius, toiminta ja turvallisuuden palauttaminen hätätilanteissa	ISO 28000:2007, luku 4.4.7
ISO 31000	Ei vaatimuksia	

Taulukko 13 Viitekehysten väliset vastaavuudet: Tominta poikkeustilanteissa

Poikkeamat, korjaavat ja ennaltaehkäisevät toimenpiteet		**Lähdeviite**
AEO	Sisäisen valvonnan menettelyt	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.6
KATAKRI	Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet	KATAKRI A604.0-A607.0
OHSAS 18001	Vaaratilanteiden tutkinta, poikkeamat, korjaavat toimenpiteet ja ehkäisevät toimenpiteet	OHSAS 18001:2007, luvut 4.5.3.1-4.5.3.2
ISO 9001	Poikkeavan tuotteen ohjaus Tiedon analysointi Korjaava toimenpide Ehkäisevä toimenpide	ISO 9001:2008, luku 8.3 ISO 9001:2008, luku 8.4 ISO 9001:2008, luku 8.5.2 ISO 9001:2008, luku 8.5.3
ISO 14001	Poikkeamat, korjaavat toimenpiteet ja ehkäisevät toimenpiteet	ISO 14001:2004, luku 4.5.3
ISO 27001	Tietoturvallisuuden hallintajärjestelmän jatkuva parantaminen Korjaavat toimenpiteet Ehkäisevät toimenpiteet	ISO 27001:2006, luku 8.1 ISO 27001:2006, luku 8.2 ISO 27001:2006, luku 8.3
ISO 28000	Turvallisuuteen liittyvät vahingot, häiriöt, poikkeamat, korjaavat ja ehkäisevät toimenpiteet	ISO 28000:2007, luku 4.5.3
ISO 31000	Ei vaatimuksia	

Taulukko 14 Viitekehysten väliset vastaavuudet: Poikkeamat, korjaavat ja ennaltaehkäisevät toimenpiteet

Suorituskyvyn mittaaminen		Lähdeviite
AEO	Sisäinen järjestely (menettelyt)	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.3
KATAKRI	Turvallisuustoiminnan tavoitteiden mittaus	KATAKRI A303.0
OHSAS 18001	Toiminnan tason mittaukset ja tarkkailu	OHSAS 18001:2007, luku 4.5.1
ISO 9001	Prosessien seuranta ja mittaus	ISO 9001:2008, luku 8.2.3
ISO 14001	Tarkkailu ja mittaukset	ISO 14001:2004, luku 4.5.1
ISO 27001	Ei vaatimuksia (HUOM. Tietoturvallisuuden hallintajärjestelmän valvominen ja katselmointi)	ISO 27001:2006, luku 4.2.3
ISO 28000	Turvallisuuden suorituskyvyn mittaukset ja tarkkailu	ISO 28000:2007, luku 4.5.1
ISO 31000	Puitteiden seuranta ja katselmointi	ISO 31000:2009, luku 4.5

Taulukko 15 Suorituskyvyn mittaaminen

Hallintajärjestelmän arviointi		Lähdeviite
AEO	Sisäisen valvonnan menettelyt	AEO Suuntaviivat 2012, liite 2. Uhat, riskit ja mahdolliset ratkaisut, luku 5.1.6
KATAKRI	Johdon katselmus: turvallisuusjärjestelmän toimivuus Vuotuisen toimintaohjelman tarkistaminen	KATAKRI A901.0 & A903 KATAKRI A203.0
OHSAS 18001	Vaatimusten täyttymisen arviointi Sisäinen auditointi	OHSAS 18001:2007, luku 4.5.2 OHSAS 18001:2007, luku 4.5.5
ISO 9001	Prosessien ja tuotteen seuranta ja mittaus Sisäinen auditointi	ISO 9001:2008, luvut 8.2.3-8.2.4 ISO 9001:2008, luvut 8.2.2
ISO 14001	Vaatimusten täyttyminen Sisäinen auditointi	ISO 14001:2004, luku 4.5.2 ISO 14001:2004, luku 4.5.5
ISO 27001	Tietoturvallisuuden hallintajärjestelmän johdon katselmus Tietoturvallisuuden hallintajärjestelmän valvominen ja katselmointi	ISO 27001:2006, luku 7 ISO 27001:2006, luku 4.2.3
ISO 28000	Järjestelmän arviointi Auditointi	ISO 28000:2007, luku 4.5.2 ISO 28000:2007, luku 4.5.5
ISO 31000	Puitteiden seuranta ja katselmointi	ISO 31000:2009, luku 4.5

Taulukko 16 Viitekehysten väliset vastaavuudet: Hallintajärjestelmän arviointi